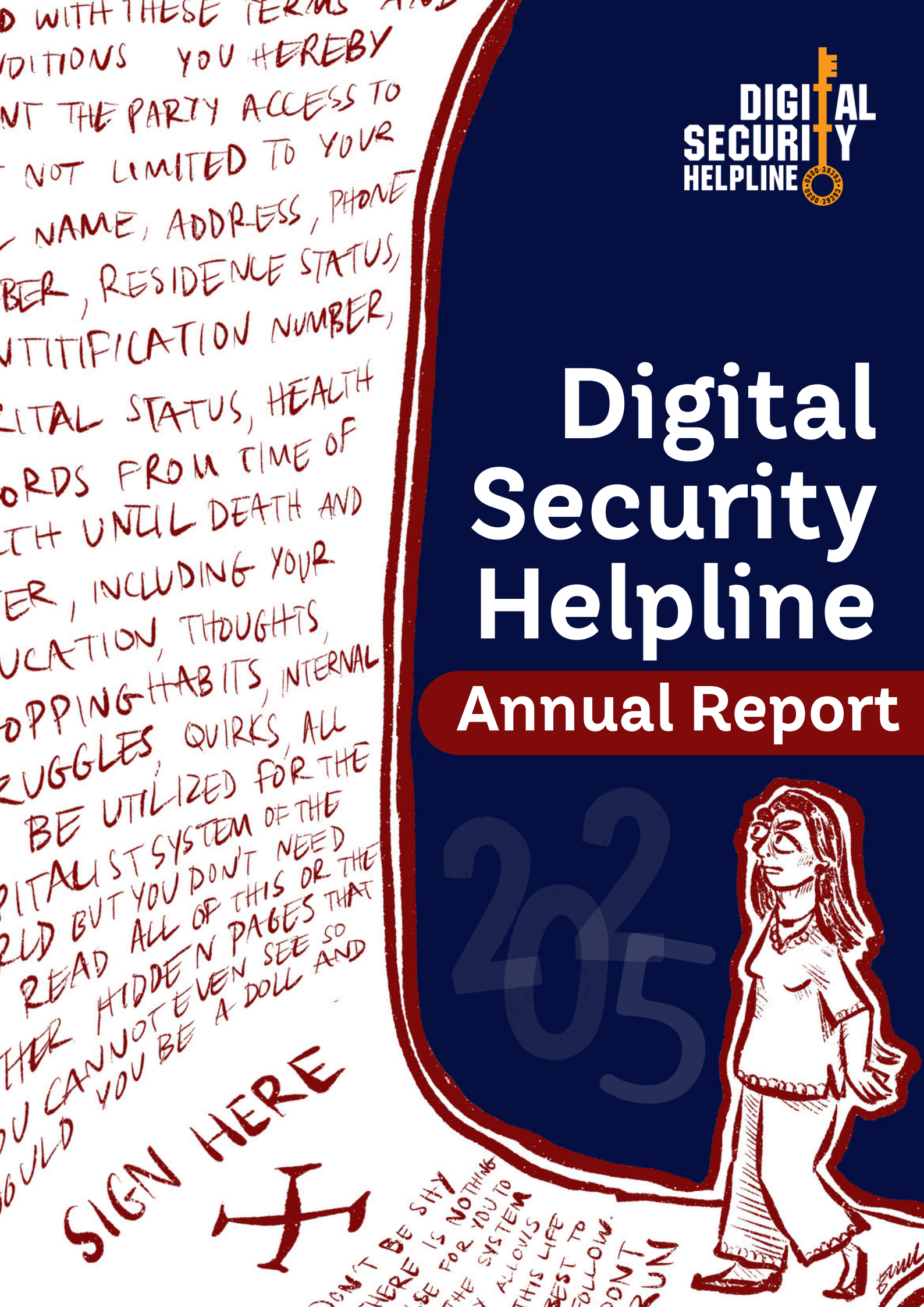
DIGITAL SECURITY HELPLINE

Digital Security Helpline

Annual Report

2025



About Digital Rights Foundation

Digital Rights Foundation (DRF) is a women-led, not-for-profit organization working since 2013 to advance digital rights and online freedoms across South Asia and the broader Global Majority. We advocate for inclusive, rights-respecting digital spaces by driving policy change through strategic engagement with relevant stakeholders. Our work focuses on making digital platforms and emerging technologies more equitable, accessible, and accountable. At the grassroots level, we empower individuals particularly women, marginalized communities, and human rights defenders with the tools and knowledge to navigate the Internet safely and assert their rights online.

Contact information:
info@digitalrightsfoundation.pk
www.digitalrightsfoundation.pk

Our gender-sensitive, confidential, and accessible digital security Helpline aims to provide callers with a safe space where they can easily share their problems regarding technology-facilitated gender based violence (TFGBV) and online violence. The Helpline can be contacted through phone, social media platforms and emails 5 days a week from 9 AM to 5 PM (GMT+5).

Helpline: 0800-39393
helpdesk@digitalrightsfoundation.pk

This report has been compiled by: Ayesha Sarwar, Anmol Sajjad, Hyra Basit
Reviewed and Edited by: Nighat Dad, Seerat Khan, Anam Baloch
Design and Layout by: Ahsan Zahid, Talha Umar
Cover page and illustrations by: Emil Hasnain

Table of Contents

05 A Note from DRF's Executive Director

08 Gendered Targets, Digital Frontlines: The Helpline's Evolving Response

11 - Our Support Services

16 Year in Review - 2025

20 Age-Specific Data Trends

22 Case in Focus: Technology-Facilitated Intimate Partner Abuse

25 Access to Justice: Local and Global Reach

30 Case in Focus: Cross-border Technology-Facilitated Harassment and Barriers to Justice

33 Gender Distribution

36 High-risk Individuals and Marginalized Communities

40 Case in Focus: Gendered Online Attacks Targeting Journalists

43 Tracking Digital Threats: Platform-Specific Trends and Advocacy Efforts

46 Gendered Dimensions of Digital Threats: Trends and Insights

Table of Contents

53 **Case in Focus: Image-Based Abuse and Its Gendered Impact**

60 **Caring for Caregivers: Supporting Incident Response Analysts**

63 **Insights into Reach and Trust**

64 - Impact Survey and Analysis

69 **Recommendations**

- Law Enforcement 44
- Social Media Platforms 47
- Policymakers

76 **Appendix 1**

A Note from DRF's Executive Director

The past year has once again demonstrated how deeply digital spaces are intertwined with people's safety, dignity, and ability to participate in public life. For women, children, journalists, and marginalized communities in Pakistan and across the region, digital spaces continue to offer important opportunities for connection, expression, and livelihood. Yet it also remains a space where harassment, intimidation, and abuse are increasingly organized, amplified, and technologically sophisticated.

In 2025, Pakistan experienced a particularly turbulent period in relation to cybercrime governance and enforcement. Ongoing debates about the amendments to the cybercrime law, and institutional changes such as the introduction of an alternate cyber crime investigation department, disrupted the country's cybercrime framework, creating uncertainty for both users and law enforcement actors responsible for addressing online harms. For victim-survivors seeking justice or protection, navigating these shifting structures often added further complexity to an already difficult process. In such an environment, independent support systems become even more essential.

For almost a decade now, the Digital Security Helpline has worked to fill this gap. Even in times of institutional uncertainty, we have remained committed to sustaining the Helpline as a lifeline for individuals facing technology-facilitated harm. Every day, survivors reach out to us while experiencing harassment, blackmail, non-consensual image sharing, impersonation, and coordinated online attacks. Behind each case is a person navigating fear, stigma, and real-world consequences that extend far beyond the screen. Our role has been to provide not only technical guidance and platform support, but also empathy, clarity, and pathways to protection.

At the same time, the Helpline's work increasingly reflects the cross-border nature of digital harms. In the past year, we have continued to see cases originating from outside Pakistan, demonstrating the growing regional and global relevance of the service. While our roots remain grounded in Pakistan, the challenges faced by users across South Asia and beyond often mirror one another. This has reinforced the importance of strengthening partnerships across borders to address online harms collectively; this year, we

were at the forefront of knowledge sharing practices with several up-coming and developed Helplines, as well as research to strengthen the collective reach of feminist Helplines.

Alongside the Helpline, we have also continued the steady development of the Emerging Threats Lab, which seeks to better understand evolving patterns of digital risk. As technology evolves, so too do the tactics used to target vulnerable individuals and communities. Artificial intelligence (AI), generative media, and automated content production are reshaping the landscape of online harm. From synthetic imagery to increasingly sophisticated forms of impersonation and harassment, these technologies present new challenges for both platforms and those working to support survivors.

Responding to these developments requires us to become more sophisticated in our own approaches to complaint handling, digital investigations, and harm mitigation. At the same time, we must explore how these very technologies can be used responsibly, even within the Helpline, to strengthen support systems, improve early detection of threats, and enhance survivor assistance. In other words, the challenge before us is not only to respond to the risks posed by AI-driven harms, but also to learn how to make these tools work for the safety of users rather than against them.

Despite the challenges, there are also important reasons for optimism. Over the past year, we have seen growing national and international recognition of technology-facilitated gender-based violence (TFGBV) and the urgent need for coordinated responses. Civil society organizations, researchers, policymakers, and platforms are increasingly acknowledging that online harms are not isolated digital incidents but part of broader patterns of discrimination, violence, and exclusion.

As this report shows, the work of the Digital Security Helpline remains rooted in the experiences of the people who reach out to us every day. Their stories remind us why sustained investment in survivor-centered support systems is essential. They also underscore the importance of collaboration between civil society, technology platforms, policymakers, and communities to build safer and more equitable digital environments.

In the years ahead, our commitment remains clear: to ensure that those facing digital harm are not left to navigate these challenges alone, and that the Helpline continues to serve as a trusted lifeline for individuals seeking safety, support, and accountability in an increasingly complex digital world.

Nighat Dad,
Executive Director
Digital Rights Foundation

Gendered Targets, Digital Frontlines: The Helpline's Evolving Response

In 2025, Pakistan was ranked 148th out of 148 countries in the World Economic Forum's Global Gender Gap Report,[1] with an overall gender parity score of just 56.7%. The drop in ranking from the previous year reflects long-standing gender disparities in economic and political participation, access to education and health services, highlighting the deepening structural gender gap issue in the country.

While these structural inequalities are commonly found in physical spaces, they also permeate online and are reflected in access to digital technology and the internet. According to the GSMA Mobile Gender Gap Report 2025,[2] only 45% of women in Pakistan used mobile internet in 2024, while device ownership gaps persist: 58% of women own a mobile phone compared to 93% of men. One of the major reasons for this persisting gender gap over the years is the lack of family approval and restrictions on how and when women are allowed to use the mobile internet. These barriers, when combined with patriarchal norms that infringe on women's basic rights and weak accountability mechanisms, create conditions in which technology-facilitated gender-based violence (TFGBV) thrives.

Globally, a study published by UN Women in 2025,[3] found that 70% of women in public life have experienced online violence, with a growing proportion reporting that digital abuse escalated into offline consequences such as physical assault, stalking, and threats. For women journalists, the link between online harassment and physical attacks has more than doubled in just five years. The rise of Artificial Intelligence (AI) has further intensified these risks: nearly one in four women reported experiencing AI-assisted abuse, including deepfakes, voice modulation, and manipulated content designed to shame, silence, or discredit them. In Pakistan, this digital hostility intersects with one of the most challenging press environments in recent years. According to the 2025 World Press Freedom Index,[4] Pakistan's global rank fell to 158th out of 180 countries, a decline from 152nd in 2024, reflecting the increasing threats to press freedom, independence, and the safety of journalists and media practitioners, mostly driven by misuse of the Prevention of Electronic Crimes Act 2016 (PECA).

---

1. World Economic Forum. 2025. "Global Gender Gap Report 2025." World Economic Forum. June 11, 2025. https://www.weforum.org/publications/global-gender-gap-report-2025/
2. "Gender Gap." 2026. GSMA. January 16, 2026. https://www.gsma.com/gender-gap/
3. "Tipping Point: The Chilling Escalation of Violence against Women in the Public Sphere." 2025. UN Women – Headquarters. December 9, 2025. https://www.unwomen.org/en/digital-library/publications/2025/12/tipping-point-the-chilling-escalation-of-violence-against-women-in-the-public-sphere-in-the-age-of-ai
4. Commonwealth Journalists Association.2025. "Media Freedom Report Spells out the Deepening Struggle in Pakistan - c J A." C J a - Commonwealth Journalists Association. August 23, 2025. https://www.commonwealthjournalists.org/pak/

These disturbingly alarming rankings come as no surprise in a country where, in 2024, a 17-year-old[5] content creator, Sana Yousuf, was murdered for refusing a proposal. Following the incident, social media was flooded with praise for her murderer. As per Digital Rights Foundation's (DRF) case study[6] analyzing comments across social media platforms, comments posted implied that Yousuf's social media presence itself was immoral conduct and "justified" the attack under conservative patriarchal norms, propagating incorrect or exaggerated allegations based on misogynistic stereotypes, gendered hate speech, and disinformation that places the responsibility on the victim's behavior or character rather than on the offender.

The state of religious freedom[7] in Pakistan has also deteriorated significantly, with social media and messaging platforms routinely being used to circulate sectarian rhetoric, hateful posts, and false accusations that target minority communities. These digital tactics are not limited to online spaces; they frequently contribute to offline mob violence, intimidation, and discrimination against religious minorities. Members of minority groups have been constrained in their capacity to engage freely and safely in both digital and public life due to the ongoing threat of online hate, which includes vilification and incitement to violence.

Transgender and gender-diverse individuals in Pakistan experience technology-facilitated abuse that is often intensely personal, targeted, and quick to escalate into offline danger. In one documented case from Peshawar,[8] a transgender woman was impersonated and used to solicit money from strangers, resulting in threats and a man arriving at her residence with a weapon. Similarly, transgender individuals[9] in Pakistan are often the targets of organized online hate campaigns, with coordinated harassment online contributing to serious threats to their safety and legal rights.

Pakistan's digital landscape has also increasingly been misused to facilitate more severe forms of harm, including organized child sexual exploitation. In Rawalpindi,[10] the National Cyber Crime Investigation Agency (NCCIA) uncovered a grooming and

---

5. Images. 2025. "Worst Place to Be a Woman': Internet Reacts as Pakistan Hits Rock Bottom in WEF's Gender Gap Report." Images. June 13, 2025. https://images.dawn.com/news/1193733
6. Digital Rights Foundation. 2025. "Case Study: Viral Misogyny and the Killing of Sana Yousaf." Digital Rights Foundation. https://digitalrightsfoundation.pk/wp-content/uploads/2025/06/Case-Study-Viral-Misogyny-and-the-Killing-of-Sana-Yousaf.pdf
7. CSOH. 2025. "Systemic Persecution of Religious Minorities in Pakistan." Center for the Study of Organized Hate. August 18, 2025. https://www.csohate.org/2025/08/17/religious-minorities-in-pakistan/
8. Afridi, Islam Gul, and Islam Gul Afridi. 2025."She Danced Online and He Came with a Gun - Digital Rights Monitor." Digital Rights Monitor. July 24, 2025. https://digitalrightsmonitor.pk/socialmediaprofiles-turned-deadly-trans-cyber-harassment-kp/
9. Shazeen Saeed. 2025. "Online Hate Isn't Just Virtual for Transgender Women in Pakistan— It's Lethal - Digital Rights Monitor." Digital Rights Monitor. October 10, 2025. https://digitalrightsmonitor.pk/online-hate-isnt-just-virtual-for-transgender-women-in-pakistan-its-lethal/
10. Asghar, Mohammad. 2026. "Child Exploitation Network Uncovered, Key Suspect Held." Dawn. February 2, 2026. https://www.dawn.com/news/1970458

blackmail network in which a suspect allegedly posed as a girl through fake Instagram accounts, deceived minors into sharing intimate material, and then extorted them by threatening to circulate the content. More than 600 indecent videos were recovered from his devices, with evidence of the sharing and trade of child sexual abuse material across social media. Authorities also uncovered and dismantled an international child sexual exploitation ring operating out of a gaming club in Muzaffargarh,[11] Punjab, where children aged 6 to 10 were reportedly lured, abused, and filmed for distribution on encrypted platforms and the dark web. These cases demonstrate how digital tools such as impersonation, encrypted communication, and cross-border networks are being deployed for organized abuse against children.

In light of rapidly growing threats posed by technology-facilitated harassment to people's safety, dignity, and lives, both online and offline, the need for accessible, survivor-centered support mechanisms like the Digital Security Helpline became increasingly important. The Helpline was launched in 2016 as a response to repeated requests for support from users, especially young girls, who experienced online abuse during DRF's Hamara Internet trainings on digital safety and internet use. The same year, the murder of Qandeel Baloch,[12] who rose to popularity because of her social media persona, brought global attention to the deadly intersections of online harassment and offline violence. It also brought attention to the urgent need for holistic support mechanisms that comprise legal assistance, emotional care, and digital security.

Over the years, we have expanded the scope of our service to align with the needs of the people we aim to help. To reflect the very specific and specialized service we provide, we have updated our title from Cyber Harassment Helpline to Digital Security Helpline, as we now include an Emerging Threat Lab in South Asia in our scope of work alongside addressing the most sophisticated digital attacks against civil society organizations (CSOs), human rights defenders (HRDs), and journalists. The Helpline's continued work is anchored in the recognition that control over digital identity is essential to inclusion, safety, and dignity in an increasingly connected world and that supporting a safer internet requires adaptive, research-informed, and survivor-centered policy adaptations.

11. Ahmed, Ashfaq. 2025. "Dark Web: Pakistan Busts Global Child Abuse Ring Operating from 'Gaming Club.'" Gulf News. June 4, 2025.
12. Mohsin, Moni. 2016. "The Dishonourable Killing of Qandeel Baloch." The Guardian. The Guardian. July 18, 2016. https://www.theguardian.com/lifeandstyle/2016/jul/18/dishonourable-killing-qandeel-baloch-pakistan-social-media-brother

Since its inception, the Digital Security Helpline has handled 23,032 cases (see Appendix 1), with women consistently forming the majority of those seeking assistance. Similarly, in 2025, 58% of all individuals who have reached out to the Helpline are women, highlighting the urgent need for continued advocacy and systemic change to create a safer online space.

Our Support Services

We offer a range of digital security and online protection services to help individuals safeguard their online presence and respond to cyber threats.

Account & Platform Assistance

- **Remove impersonation of accounts, groups, or fraudulent pages**
- **Reactivate accounts, groups, or pages that were wrongfully suspended.**
- **Restore hacked accounts, groups, or pages.**

Digital Security Guidance

Our incident response analysts provide personalized digital security tips and tools to help protect against:

- **Device hacking or confiscation**
- **Malware-infected devices**
- **Phishing and social engineering tactics**
- **Digital surveillance threats**
- **Data breaches and data encryption attacks**
- **AI-generated and manipulated images, videos, or audio used for deception.**

Content Removal Support

Through our Trusted Partner channels, we assist in the removal of harmful or abusive content, including:

- **Online harassment & cyberbullying**
- **Doxxing**
- **Hate speech & incitement Disinformation & defamation campaigns**
- **Sextortion & gender-based violence**
- **Content related to device theft**
- **Impersonation or identity theft**
- **Child Sexual Abuse Material (CSAM)**

Expanded Legal & Counseling Support

As a digital security and threat response Helpline, we continuously adapt and expand our services to meet the evolving needs of our callers. Our efforts go beyond immediate assistance; we strive to provide long-term, holistic support through legal aid, counseling, and advocacy.

Total Number of Calls attended by the Legal Team — **143**

Total Court and NCCIA Visits — **30**

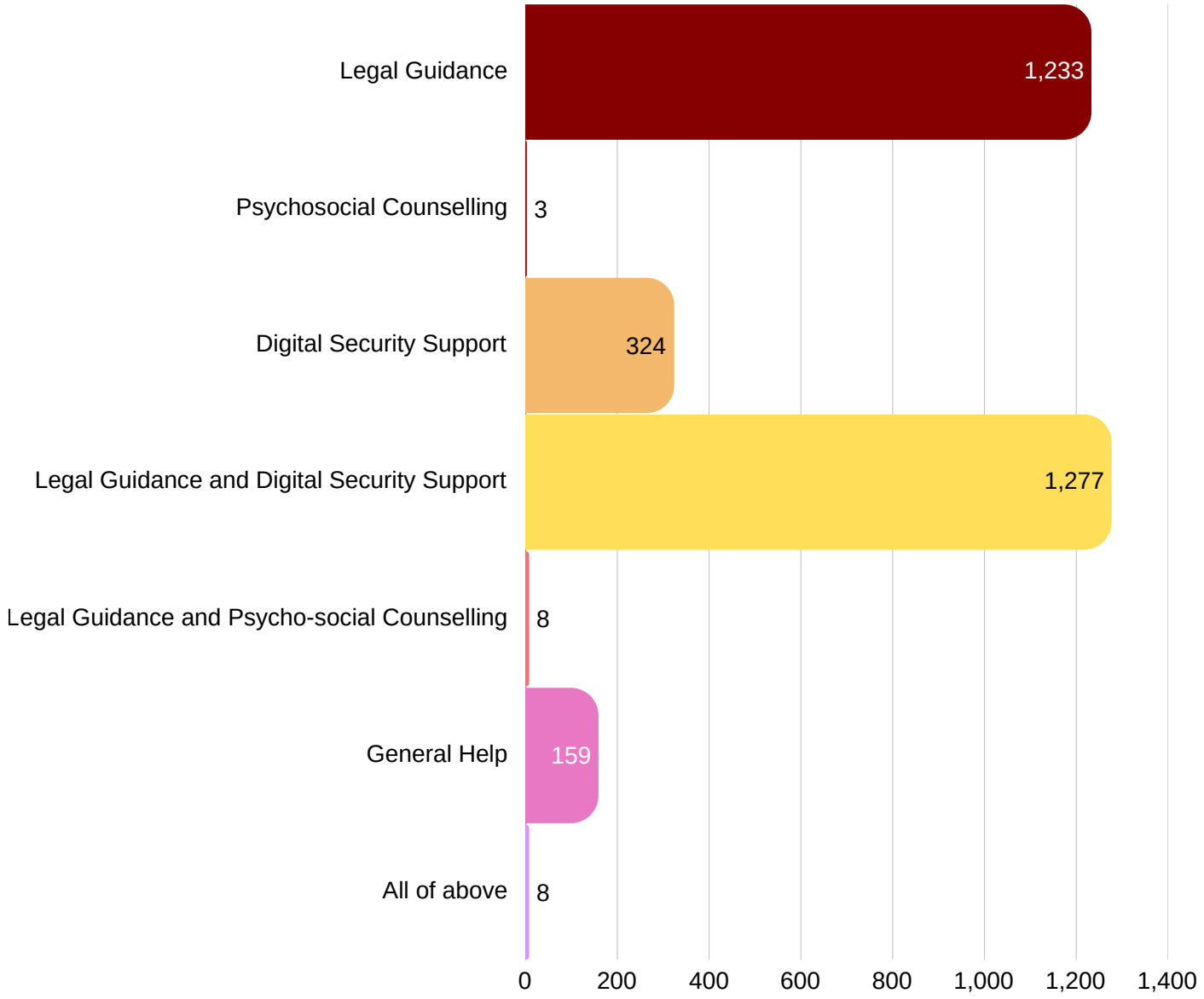
Total Number of Survivors Assisted — **68**

- Our online legal directory, 'Ab Aur Nahin,' connects individuals with pro bono lawyers across the country, offering free legal assistance for those facing tech-facilitated gender-based violence and digital threats.

- We also provide in-person counseling and legal aid for individuals filing cybercrime complaints with NCCIA's office in Lahore, Karachi, and Islamabad, ensuring they receive guidance throughout the legal process.

Mental Health and Psycho-social Well-being

Oftentimes, the Helpline is the first and only support available to vulnerable individuals, especially women, children, and religious and gender minorities - individuals who fear being victim-blamed or face harsh repercussions based on their identity, either from their families or law enforcement. We recognize the sensitivity of digital security cases and prioritize the confidentiality and protection of our callers' information. The Helpline's strict data privacy protocols ensure that personal details are collected only when absolutely necessary, based on the nature of the case, and that they then remain secure and undisclosed to any third party. Furthermore, our team is trained to handle cases with discretion and professionalism, creating a safe and supportive space for individuals seeking help. Feedback received from our beneficiaries often highlights the non-judgemental, supportive, and calm response received from the Helpline when seeking support.



Awareness & Capacity Building

Throughout the year, DRF's Digital Security Helpline reached 354 students of all ages across Pakistan through a series of awareness and capacity-building sessions. Our training series covered foundational discussions on gender, patriarchy, and consent, as well as more advanced conversations on emerging trends in online abuse and digital threats. Our outreach spanned multiple cities and regions, including Karachi, Lahore, Gilgit-Baltistan, Kashmir, Multan, and Hyderabad.

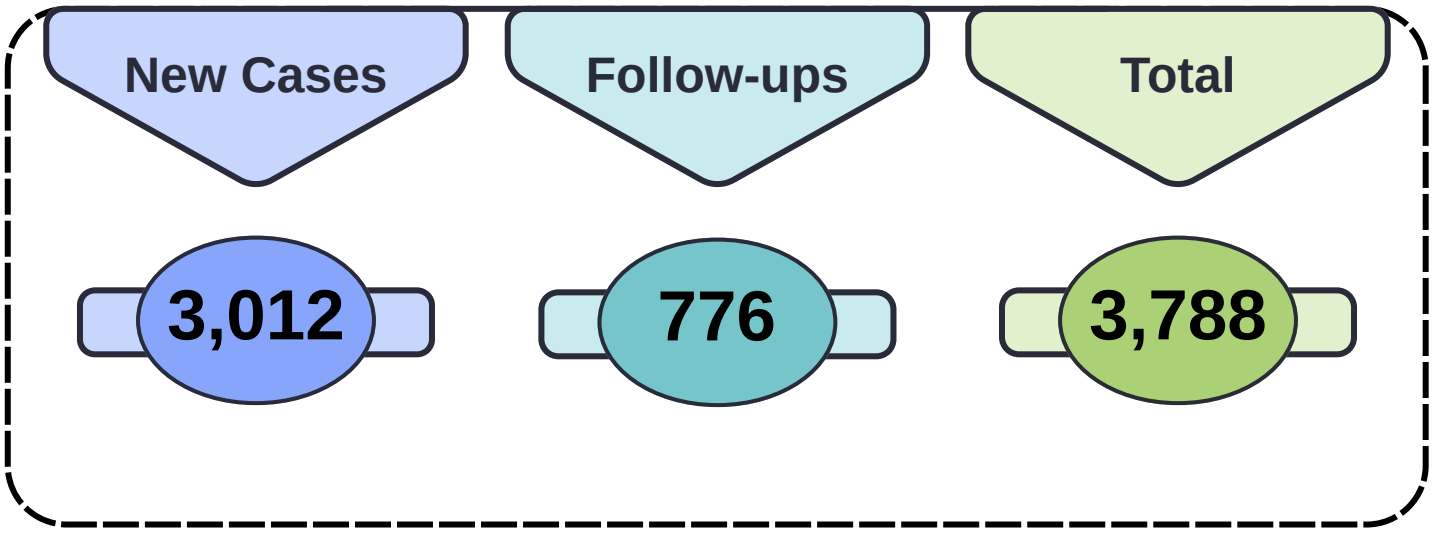
One of the most impactful visits was to Hunza, where we conducted sessions with a local girls' college and received an overwhelmingly positive response, particularly in terms of how helpful the session was for online safety and privacy tips. Our experience there reinforced how essential our outreach is in remote regions, particularly where access to justice and awareness on digital safety is limited.
In addition, the Helpline has been part of all the sessions conducted by the DRF team as part of the Digital Safety and Literacy Sessions[13] for Young Adults (Hamara Internet, Mahfooz Internet) training program on TFGBV. The DRF team for this program visited 16 primary government schools in different areas of Lahore. These sessions engaged a total of 2,857 students, including 1,485 girls and 1,372 boys between the ages of 13 to 18.

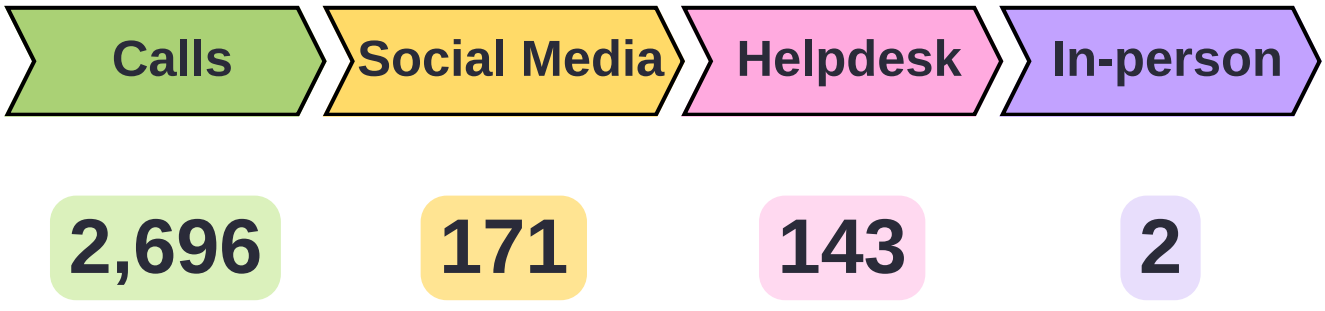
These sessions were designed to build long-term awareness around digital safety for students and educators and equip them with practical tools to respond effectively. By engaging teachers at the same time as students, DRF's program team aimed to involve all stakeholders and build an ecosystem of support for all. The Helpline frequently receives cases from young adults, particularly pertaining to online violence. Due to the lack of violence and institutional support for these young adults, many develop severe mental health issues at a young age, which are extremely important to address. Through the Hamara Internet program by involving teachers in our campaign, we hoped to build a relationship of trust and equip them with the emotional and practical tools to support their students.

13. Digital Rights Foundation. 2023. "Digital Rights Foundation and Deputy Commissioner Lahore District Administration sign a MoU to conduct Hamara Internet Mahfooz Internet Digital Literacy and Safety Sessions." Digital Rights Foundation. https://digitalrightsfoundation.pk/digital-rights-foundation-and-deputy-commissioner-lahore-district-administration-sign-a-mou-to-conduct-hamara-internet-mahfooz-internet-digital-literacy-and-safety-sessions/

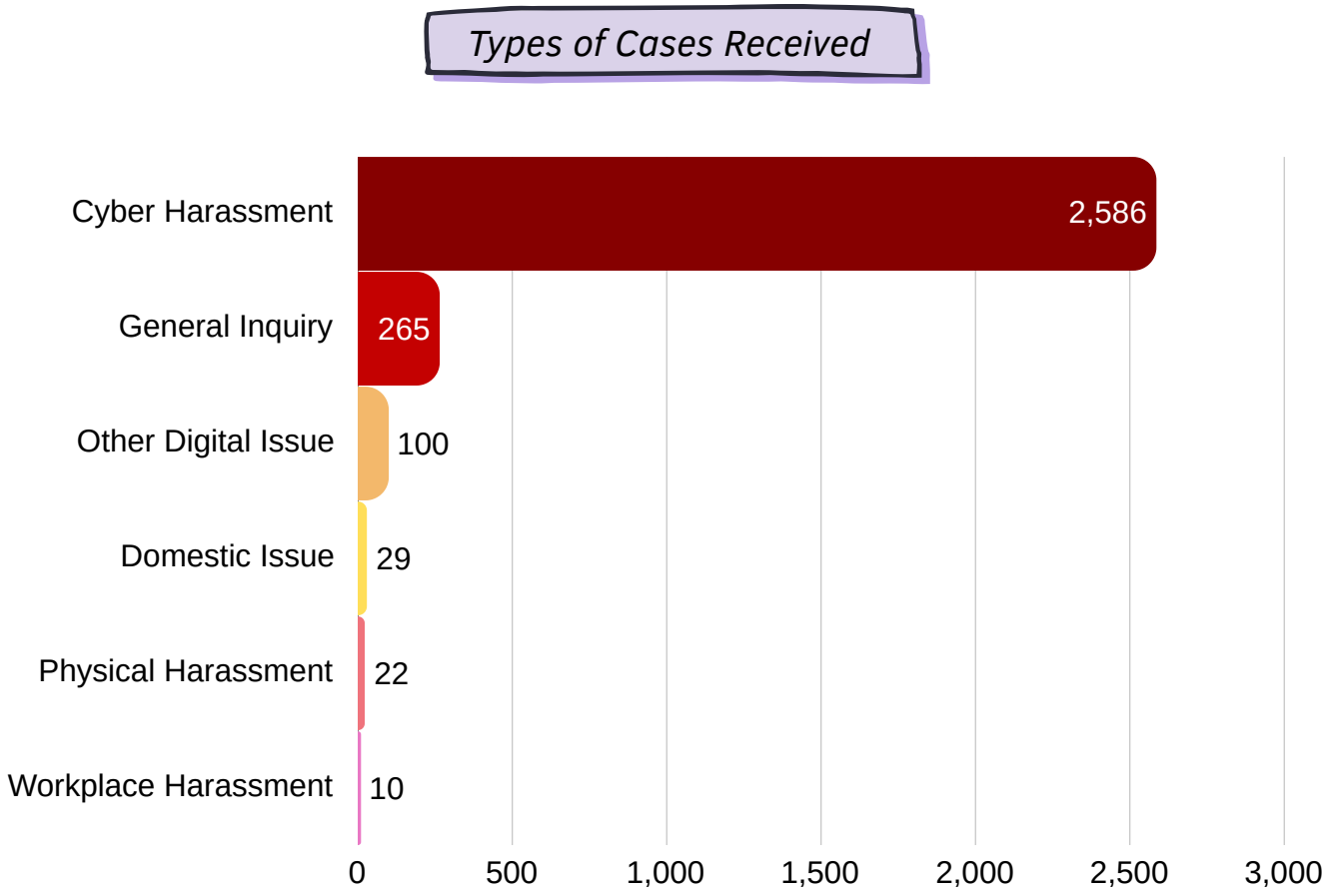
Year in Review - 2025

Consistent with patterns seen in previous years, the Helpline received a total of 3,012 cases in 2025. The Digital Security Helpline receives cases primarily through three channels of communication: the Helpdesk email, the Helpline landline service, and social media chat services. The majority of incidents, 2,696 in total, were reported via the Helpline landline, reinforcing its role as the primary point of contact for victim-survivors. While speaking directly to our beneficiaries enables us to build a relationship of trust in real time, the Helpdesk and social media chat services allow us to reach beneficiaries who may not have sufficient privacy or are not based in Pakistan.





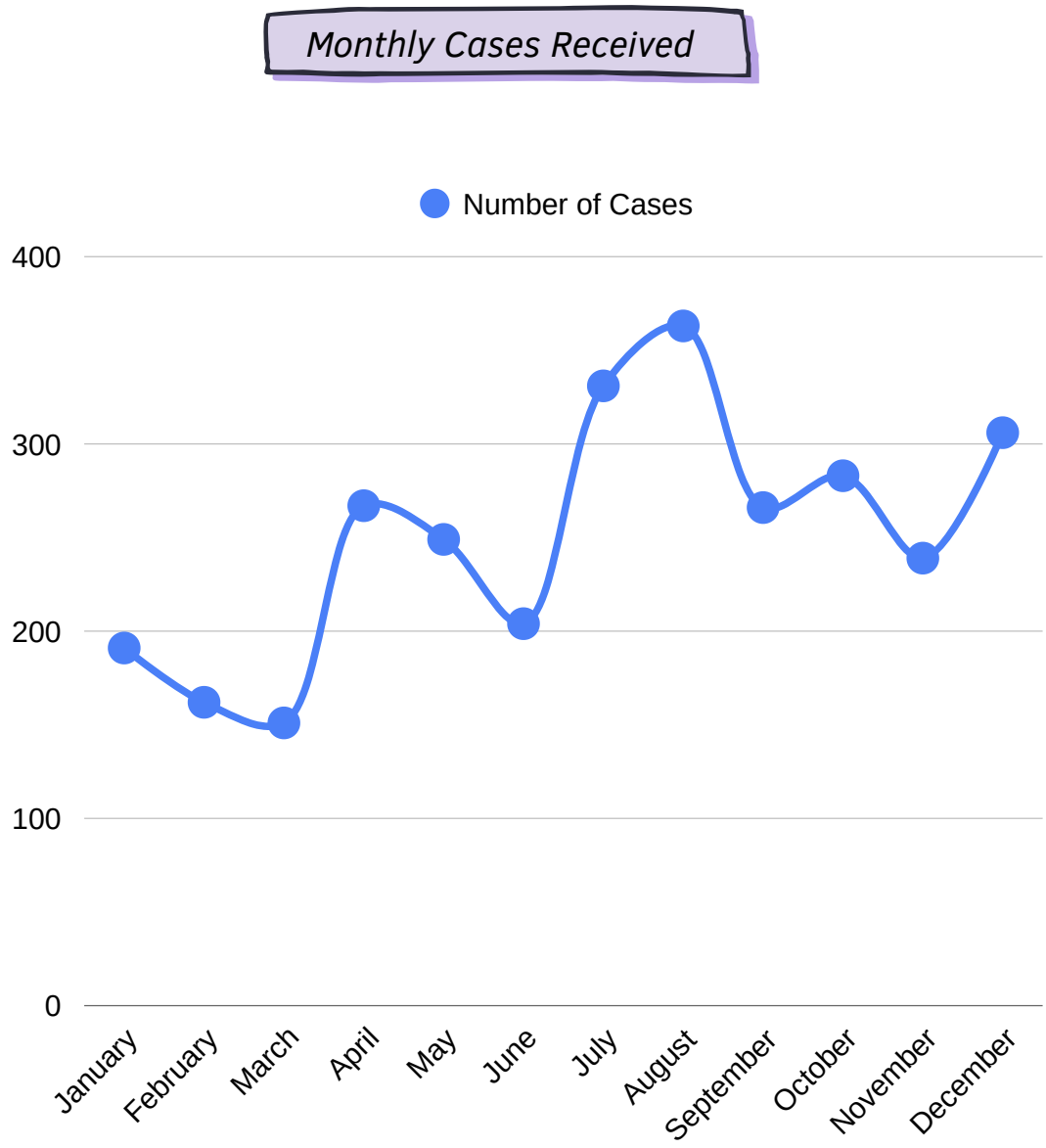
Although the Helpline focuses on cases of technology-facilitated violence, other complaints are also entertained depending on capacity, given the intersection of online harassment with other forms of violence. An average of 250 new cases were received each month.



During the reporting period, we observed various trends wherein AI-generated content overlapped with misinformation and disinformation. During the September 2025 flood crisis,[14] AI-generated images and videos circulated widely that threatened relief operations and were used to further political propaganda. Moreover, during this time, one of the most concerning and relevant content identified by DRF was the hyper-sexualized imagery of women as distressed victims of the floods. DRF also monitored online spaces during the conflict between India and Pakistan, particularly when TFGBV was on the rise and hyper masculine narratives, along with AI slop, flooded platforms against women and gendered minorities from both sides of the border. [15]

14. Digital Rights Foundation. 2025. “Combatting Flood Misinformation in Pakistan.” Digital Rights Foundation.https://digitalrightsfoundation.pk/wp-content/uploads/2025/09/Combatting-Flood-Misinformation-in-Pakistan.pdf
15. Digital Rights Foundation. 2025. “Digital Battlegrounds: Gendered Disinformation, TFGBV,, and Hate Speech in the Indo-Pak Escalations.” Digital Rights Foundation. https://digitalrightsfoundation.pk/wp-content/uploads/2025/05/Digital-Battlegrounds-Report.pdf.

Additionally, in 2025, 17-year-old content creator Sana Yousaf was murdered[16] in Islamabad for allegedly rejecting repeated advances from a man. After Sana's death, platforms were flooded with graphic content and praise for her killer. This particular case highlights the escalating risks and abuse faced by women on online platforms in Pakistan. Similarly, earlier in the year in Quetta,[17] a father confessed to killing his 15-year-old daughter over her social media account activity, namely TikTok, citing objections to her online presence. In another incident, a father shot dead his daughter over her refusal to delete[18] her TikTok account/application from her phone. Law enforcement agencies cited honor killing as the motivation behind this murder, highlighting how women's dignity and perceived association with family honor continue to be policed and contested, now extending to their online activity and digital presence.

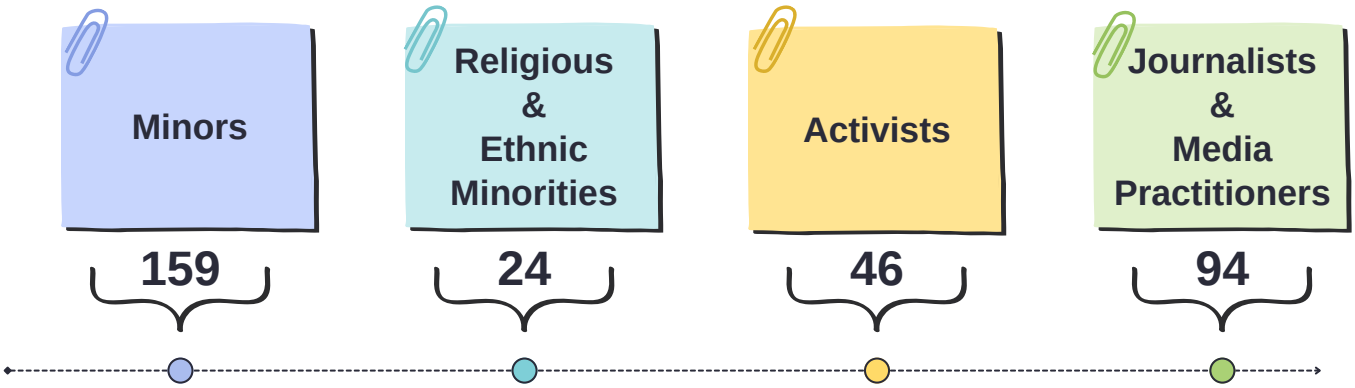


16. Shamim, Sarah. 2025. "Who Was Sana Yousaf, Pakistani TikTok Star Shot Dead by a Gunman?" Al Jazeera. June 4, 2025. https://www.aljazeera.com/news/2025/6/4/who-was-sana-yousaf-pakistani-tiktok-star-shot-dead-by-a-gunman
17. Ng, Kelly. 2025. "Pakistan: US Teen Shot Dead by Father over TikTok Videos." BBC, January 30, 2025. https://www.bbc.com/news/articles/cy8pvw3xxxeo
18. "Father Kills Teen Daughter after She Refused to Delete TikTok Account, Pakistan Police Say." 2025. Cbsnews.com. July 11, 2025. https://www.cbsnews.com/news/father-kills-daughter-tiktok-account-pakistan-police/

In 2025, the Digital Security Helpline continued to receive complaints related to financial fraud, WhatsApp hacking, and harassment over digital loan applications. This year, DRF's Helpline facilitated many renowned activists and journalists when they lost access to their WhatsApp accounts. These hacked WhatsApp accounts later swindled money from their contact lists. Evolving social engineering tactics, combined with low digital literacy levels and risk awareness, along with the possibility of data breaches allows scammers to know personal details of their victims, which is a cause of concern in this digital age. A notable example involved Dr. Nikhat Shakeel,[19] a parliamentary secretary for the Ministry of Science and Technology, who fell victim to such a scam, resulting in a financial loss of Rs 1.5 million for her close circle.[20] Although the helpline did not receive this particular case, it is still an important one since it showcases broader trends of how financial fraud can target anyone and cause significant harm.

Moreover, the helpline report in 2023 documented the rise of predatory loan shark apps that exploited users' personal data, including contact lists, identification documents, and photo galleries, to coerce repayments through threats, intimidation, and public shaming. With the rise in these loan shark application cases, regulatory warnings and strict enforcement actions by the Federal Investigation Agency (FIA) and the Pakistan Telecommunication Authority (PTA),[21] led to a temporary decline in reported cases. However, cases received by the Helpline this year suggest a resurgence of similar apps, highlighting the cyclical and evolving nature of harmful digital practices.

Cases Involving High-Risk Individuals



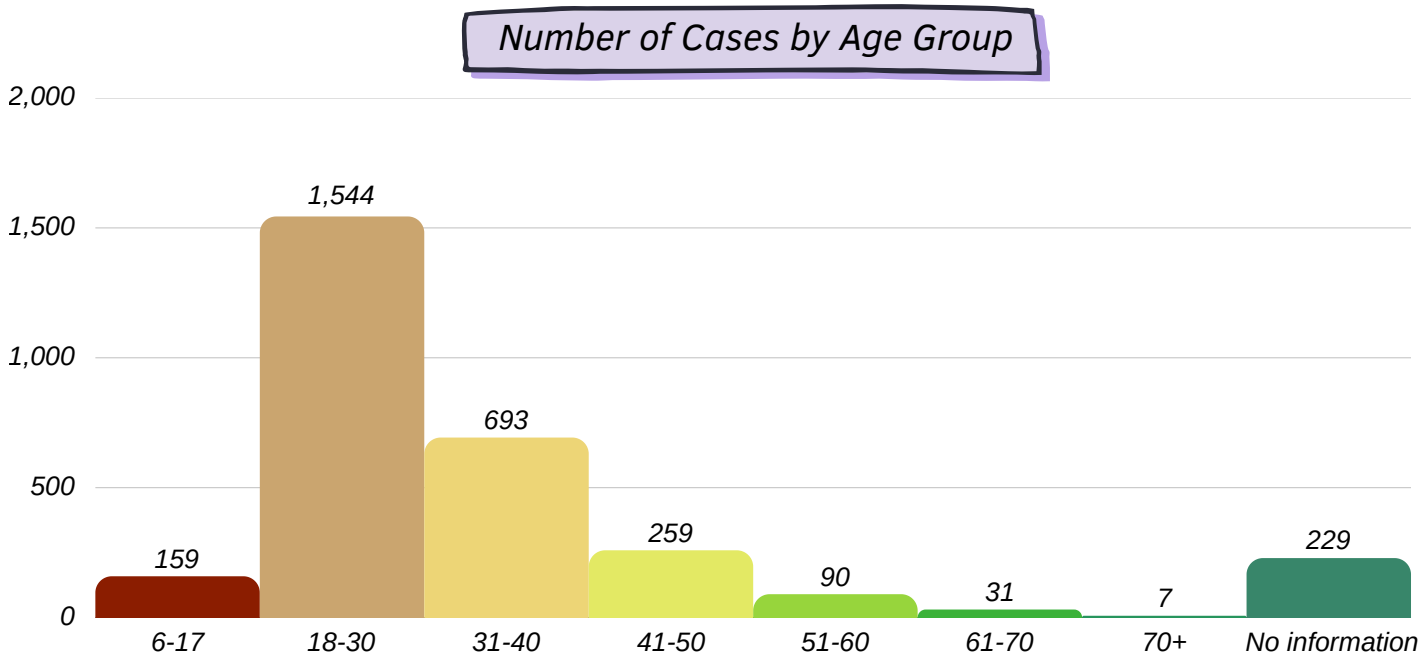
19. Digital Rights Foundation. 2025. "Case Study: MQM Politician Falls Victim to online scam." Digital Rights Foundation. https://digitalrightsfoundation.pk/mqm-p-politician-falls-victim-to-online-scam/
20. Web Desk. 2025. "ARY NEWS." Arynews.tv. ARY News. 2025. https://arynews.tv/nikhat-shakeel-of-mqm-pakistan-faces-online-scam-viral
21. "PTA Blocks 43 Unregistered Lending Apps." 2023. Dunya News. July 18, 2023. https://dunyanews.tv/en/Pakistan/740516-PTA-blocks-43-unregistered-lending-apps

Over the years, as the digital and online landscape evolved, the Helpline increased its focus on providing more holistic security to the most vulnerable and marginalized populations in society. DRF's direct and targeted approach towards outreach to these communities, in conjunction with our extensive networks developed over the years (such as the Network of Women Journalists for Digital Rights), aids us in going above and beyond just providing reactionary and situational support. The DRF team engages in awareness raising through campaigns, education and training, technical support, and regular advocacy work with various stakeholders that equips members of these communities to preemptively safeguard themselves and for their concerns to be heard more widely.

Age-Specific Data Trends

In 2025, the Helpline extended its services to individuals across a wide age spectrum, ranging from children as young as 6 years old to senior citizens above the age of 70. Out of a total of 3,012 cases received during the year, minors (under the age of 18) accounted for 159 cases (5.3%), marking a 28% increase from last year. This includes 5 cases involving children between the ages of 6 to 9.

The majority of complainants fell within the 18 to 30 age group, representing 51.3% of all reported complaints. The higher reporting rate among young adults is assumed to be linked to greater digital engagement, increased access to smartphones and social media platforms, and comparatively higher awareness of reporting mechanisms. Within this demographic, women constituted a significant proportion of those who reached out to the Helpline, reflecting the gendered nature of online harassment and technology-facilitated abuse.



Of particular concern are the cases involving children aged 6 to 9. Although these cases represent a small proportion of total complaints (0.23%), they highlight severe risks, including online grooming, sexual abuse, and digital exploitation. One case received on the helpline, for example, involved a 6-year-old girl whose pictures were posted on a social media account, and messages from this fake account were being sent to family members to defame her. In another case, an 8-year-old girl mistakenly shared family pictures with a stranger online; the perpetrator then created a fake social media profile in her name and attempted to coerce her into sharing her intimate images. Even though the number of cases is few, perhaps because of a lack of knowledge about the Helpline or other remedial options, these incidents reflect the increasing digital exposure of minors and the urgent need for parental supervision, digital literacy, and child safety awareness programs at educational institutions and at home.

Case in Focus:
Technology-Facilitated Intimate Partner Abuse

Every year, the Helpline receives numerous TFGBV cases, most of which involve vulnerable groups. To provide a deeper understanding, DRF's Helpline team spoke to a complainant, who identified herself as a woman, and shared her experience of being blackmailed, doxed, and publicly harassed, including the non-consensual posting of her pictures and contact number online. The complainant described the trauma she faced throughout the process and how the NCCIA responded to her case.

Case description:

A 41-year-old woman from Lahore was being blackmailed and harassed by her ex-partner. He repeatedly pressured her to stay in a relationship and publicly posted her personal pictures on TikTok with inappropriate songs and defamatory captions. Additionally, he created fake profiles using her contact number, which led to her receiving numerous threatening and unwanted phone calls from strangers. The harasser also threatened to tarnish her reputation if she did not agree to marry him. She experienced both doxxing and sustained blackmail. The complainant pursued legal action by filing a case with the NCCIA in Lahore.

Transcription: *During my relationship, I sometimes felt unsafe and emotionally uncomfortable with him. I felt he was toxic, which is why I eventually ended the relationship. About a month later,* ***I came across a post with my picture and contact number shared publicly,*** *along with defamatory captions. He called me slurs and labelled me a "call girl." That is when I realized he was behind it. Seeing that post made my mind go blank; I could not think clearly, and I felt completely shattered.*

At first, I did not know what to do. I kept begging him to remove the posts. I did not understand the legal procedure or where to seek help. For some time, I was just trying to convince him to stop. This incident completely changed my life. ***I was mentally disturbed and emotionally broken.*** *I told my brother that I wanted to end my life because I could not bear the humiliation and fear.*

My brother supported me during my darkest moments. Without his support, I might not be here today. He was the one who first contacted the Helpline on my behalf because I was too afraid to speak. The fear of social judgment was always present. As a divorced woman, I already felt vulnerable. I kept thinking that society would blame me and believe the lies being spread. That pressure made everything more painful.

After he posted my contact number online, I started receiving numerous calls from unknown numbers. I was constantly anxious and afraid. I avoided social interaction and felt mentally exhausted. I ran to different offices repeatedly seeking help. My daily routine was disturbed, and I was living in constant stress.

My brother was already aware of the Helpline, so he contacted them first. Initially, I was hesitant and scared to speak openly, but the Helpline team made me feel comfortable. They gave me space and time to explain everything. They provided digital support and legal guidance. They guided us step by step on how to file a complaint with the NCCIA and supported us throughout the procedure.

We filed a complaint with the NCCIA. We faced difficulties in submitting the application because we were unaware of the proper procedure. Although the case was registered, the harassment did not stop immediately. He continued posting my pictures from different accounts. This was very discouraging and affected my morale, but I kept reminding myself to stay strong. After continuous follow-ups and support, action was taken, and efforts were made to remove the content from different platforms. The process was not immediate, but with support and coordination, harmful posts were addressed. The journey has been long, but there have been improvements since the case began.

If there had been faster platform responses and clearer legal guidance at the beginning, it would have reduced my trauma. Awareness about available support systems is crucial. Without my brother's support and the Helpline's assistance, I would not have survived this phase of my life. At one point, I had accepted defeat, but their encouragement gave me the strength to fight back.

Access to Justice: Local and Global Reach

The Digital Security Helpline collects data on the city and region of each complainant to provide tailored legal guidance to our beneficiaries. This ensures that complainants are well-informed about the correct complaint procedure and do not face unnecessary delays or risks while seeking justice, in addition to all the cultural and social barriers they have to navigate through.

Beyond national boundaries, the Helpline has evolved into a transnational support mechanism for digital rights protection and survivor-centered support, assisting survivors across the globe. In 2025, the Helpline received support requests from users spanning over 30 countries, in addition to Pakistan. This global reach enables the Helpline to identify cross-border patterns of online harassment and TFGBV, highlight systemic gaps in access to justice, and inform advocacy efforts at regional and international policy levels.

Reflecting the Helpline's expanding global and regional reach, the following is the regional breakdown of the 75 international cases in 2025:

North America

USA

Canada

South America

Brazil

Oceania

Australia

East Africa

Tanzania

MENA

Iraq

Saudi Arabia

UAE

Iran

Yemen

Morocco

Turkey

Kuwait

Egypt

Syria

Europe

UK

Germany

France

Spain

Sweden

Netherlands

Italy

Georgia

Ireland

South Asia

India

Bangladesh

Afghanistan

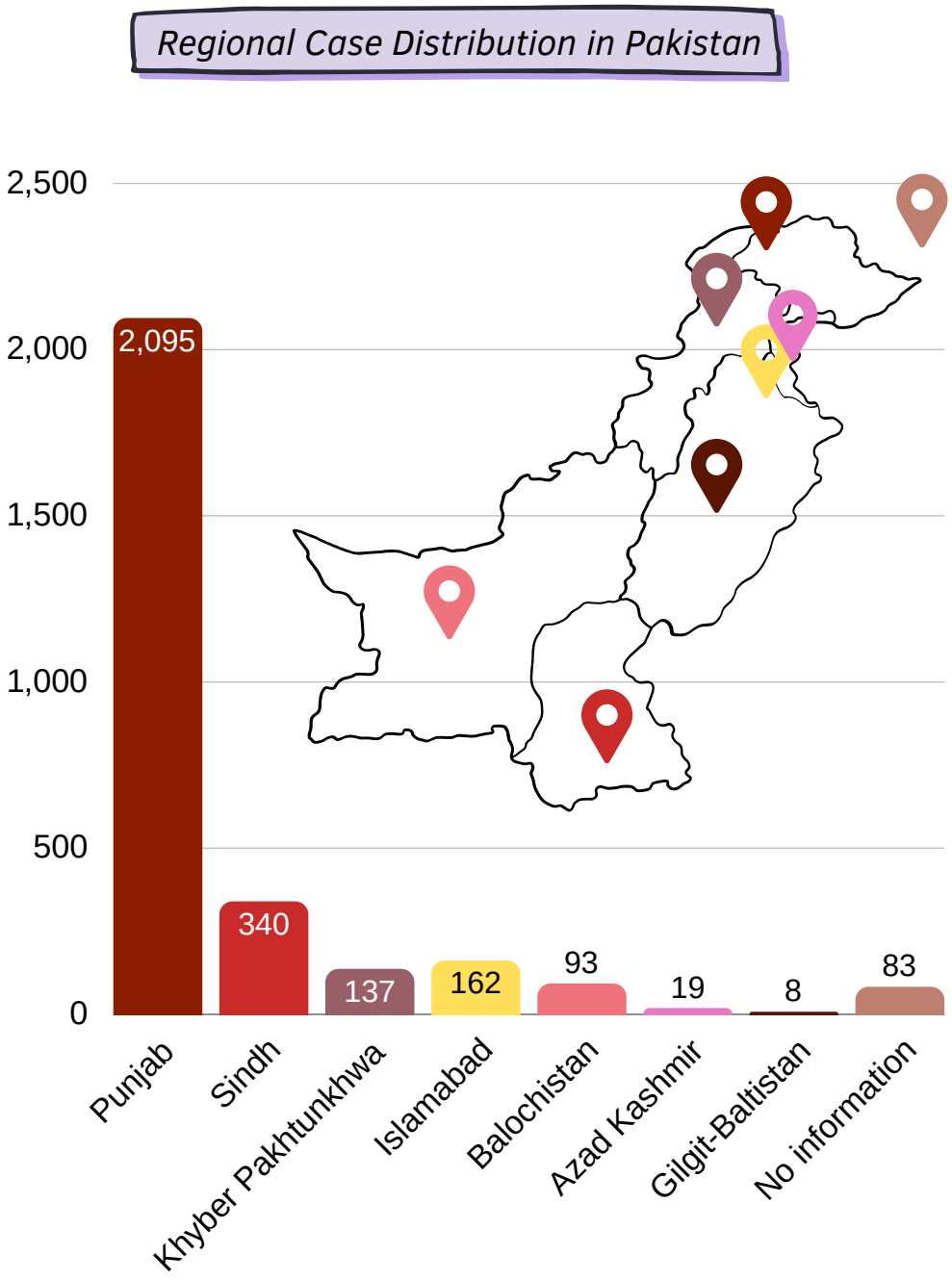
East & Southeast Asia

Malaysia

Philippines

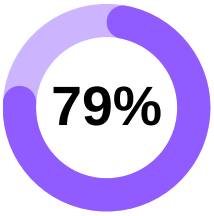
Taiwan

The distribution of cases within Pakistan continues to reflect significant regional disparities in access to justice, with rural and remote regions facing significant barriers in access to support.

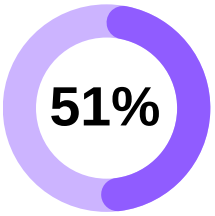


Punjab continues to report the highest number of cases (69.5%), consistent with the previous years, which is reflective of its larger population and better access to support services and the internet. Balochistan (3%) saw a lower number of cases along with Azad Kashmir (0.6%), and Gilgit-Baltistan (0.26%). This signifies that survivors in these regions are less likely to seek help due to a lack of accessibility, limited awareness, or cultural and physical constraints. The pattern of lower reporting numbers will remain persistent in these regions if these gaps are not addressed by targeted awareness campaigns to enhance digital literacy, improve digital infrastructure, and enhance legal support mechanisms.

- **Out of the 2,586 cyber harassment cases received on the Helpline, 79% were referred to the NCCIA for legal intervention.**



- **Of these total cyber harassment cases, only 51% originated from cities where an NCCIA office is operational, requiring many complainants to travel to another city to file a formal complaint.**

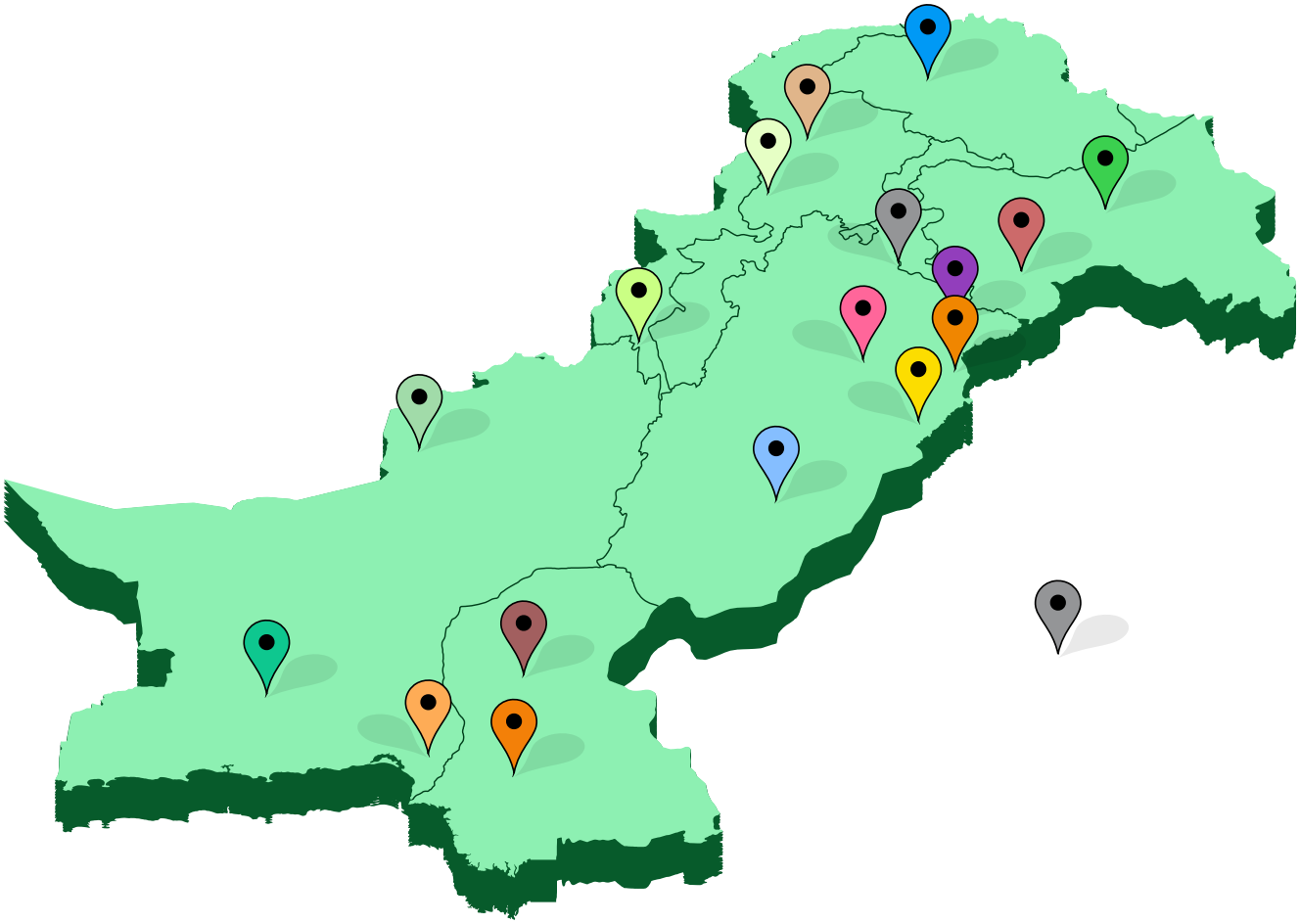


This data indicates significant accessibility challenges. Although complaints can be initiated through the NCCIA online portal, the system frequently remains unresponsive or, in rare cases of response, requires anyone wishing to pursue the complaint to physically visit the offices for verification of the complaint. For many survivors, particularly those in remote or rural areas, this procedural requirement creates an immediate and practical barrier, as NCCIA wings are only present in 15 cities spread across Pakistan. The Helpline team frequently counsels beneficiaries who have to navigate hours of travel to their nearest NCCIA office in order to seek justice.

Women, in particular, face additional constraints. For many, reporting tech-facilitated violence carries severe repercussions, particularly to their safety and social standing. Survivors frequently fear retaliation from family or community members, including shaming, isolation, loss of access to devices or mobility, and, in severe cases, ‘honor’ violence. In such contexts, engaging law enforcement without involvement from a man in the household can trigger consequences that jeopardize both the safety and livelihood of women survivors. It is significant to note that these gendered barriers prevent access to justice even in areas where NCCIA offices are located, though they are felt more prominently in underrepresented areas.

For years, DRF, as a civil society organization, has recommended decentralizing reporting mechanisms, strengthening responsive online complaint systems, and enabling remote verification processes to reduce these barriers. However, progress remains limited, and meaningful updates to accessibility and responsiveness are still urgently needed. Without such reforms, justice becomes a question of privilege aided by mobility and financial resources, particularly for women and marginalized communities, who continue to bear the greatest burden of online harm.

Cases Distribution Across Cities with NCCIA Offices



892 City without NCCIA office	**12** Abbottabad	**116** Faisalabad	**6** Gilgit	**80** Gujranwala	**1** Gwadar
28 Hyderabad	**162** Islamabad	**268** Karachi	**846** Lahore	**108** Multan	**56** Peshawar
78 Quetta	**164** Rawalpindi	**8** Sukkur	**9** DI Khan	**95** Out of jurisdiction	**83** No info

Case in Focus:

Cross-border Technology-Facilitated Harassment and Barriers to Justice

The Helpline receives frequent complaints from overseas Pakistanis facing technology-facilitated harassment that extends across borders. While PECA formally applies to all Pakistani citizens regardless of whether they reside within Pakistan or outside, its enforcement remains weak in practice. Survivors of TFGBV living abroad are often left in prolonged fear and uncertainty due to limited cross-border coordination between law enforcement agencies, which prevents timely protection for survivors and accountability for the harassers. Women disproportionately bear the consequences, including victim-blaming, character scrutiny, and restrictions on their mobility.

Case description:

The complainant identifies herself as an overseas Pakistani woman residing in the United Kingdom (UK). She added that she attempted to hold the man with whom she had been in an online relationship accountable based on the false promises he had made; however, he responded with harassment and threats. She eventually filed a complaint through the NCCIA overseas channels. The case remains under investigation with little accountability so far, while the complainant continues to face emotional and psychological distress.

Transcription: *I was in an online relationship with a man who promised me marriage. It started in 2020. During the relationship, he requested financial assistance on several occasions, which I provided in good faith, believing that he intended to formalize the relationship. He deceived me when I was vulnerable from a previous broken marriage.*

Later, I discovered that he was simultaneously in a relationship with another woman and subsequently married her, despite having previously assured me that he intended to marry me. When I began asking for repayment of the money I had transferred to him, which was a healthy sum of money, his behavior changed significantly. He became hostile, blocked communication, and began sending humiliating and threatening messages both directly and indirectly through my family members and unknown numbers. At first, I tried to resolve the matter privately. When this failed and the harassment escalated, I began preserving evidence in the form of screenshots, bank transfer records, call logs, and voice messages.

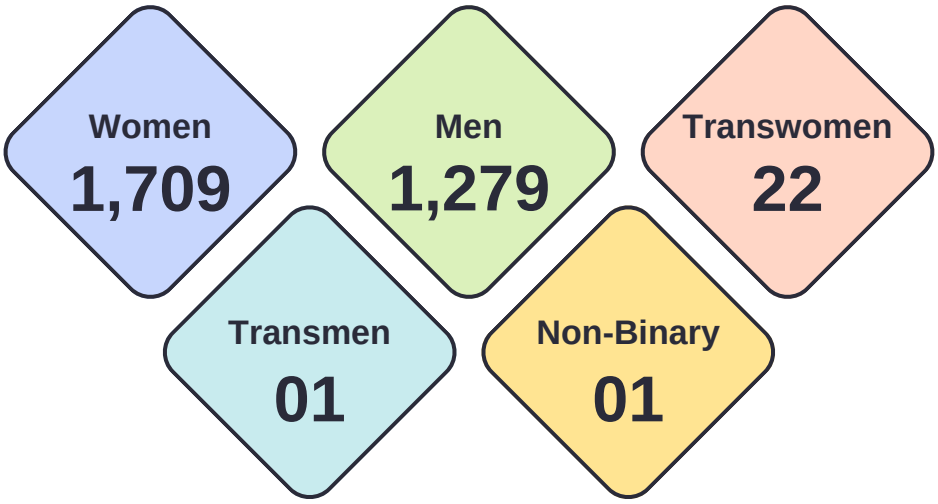
As an overseas Pakistani residing in the United Kingdom, seeking help was not straightforward. The process was not easily accessible, and there was no clear guidance on where or how to file a complaint. I had to research extensively, contact different offices, and rely on intermediaries and embassy channels to understand the procedure. During this search, I also came across the DRF's Digital Security Helpline. They guided me through the process, explained the steps involved, and helped me understand the documentation required as an overseas complainant. The Helpline also recommended relevant resources and provided emotional support at a time when I felt overwhelmed and unsure of what to do. With this guidance, I eventually filed a complaint with the NCCIA through the overseas and embassy portals and appointed a legal representative in Pakistan through a properly attested power of attorney.

The case was accepted for inquiry. NCCIA summoned the accused, seized his mobile phone for forensic analysis, recorded his statement, and froze his bank account pending investigation. While I appreciate these actions, communication regarding progress has been limited by the NCCIA, and the lack of timely updates has caused considerable stress. ***The matter is still under investigation and has not yet reached a final resolution, and to this day, receive threats and declarations of revenge from unknown numbers.***

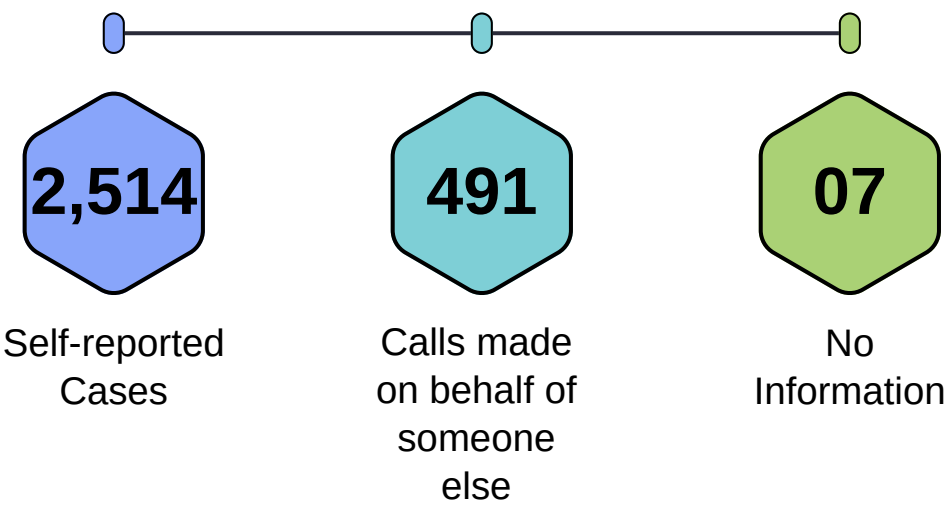
This entire experience has caused severe emotional distress, anxiety, depression, and ongoing psychological trauma. ***I am currently undergoing counseling and taking prescribed medication. The prolonged harassment, humiliation, and threats have deeply affected my sense of safety and well-being.*** *My family has also been distressed, particularly because of the fear created by threats and the uncertainty surrounding the legal process. It has disrupted my daily functioning, work, and mental health significantly.*

Navigating the Pakistani legal system from abroad while dealing with trauma has been extremely challenging. *Frequent communication and updates from investigators, clear guidance about timelines and procedures, and a dedicated liaison for overseas complainants would have made the process far less distressing. Faster responses to intimidation attempts would also have improved my sense of safety and helped with my anxiety and sense of helplessness.*

Gender Distribution

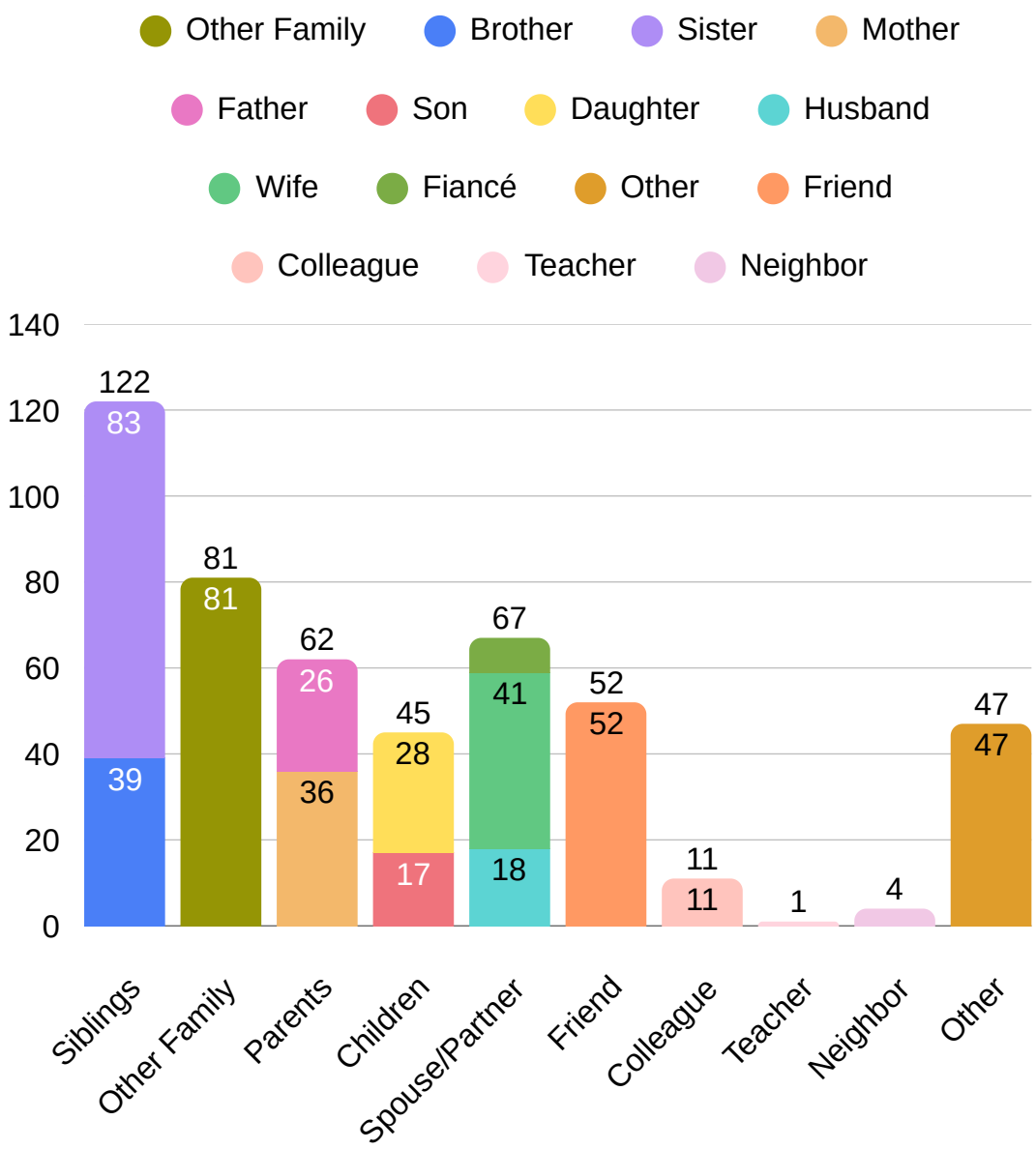


In 2016, the Helpline was launched to fill the gap that left women and girls vulnerable when they faced online violence in unsafe digital spaces. Over the years, the quantitative and qualitative data collected from the Helpline have shown that it is an essential service in this day and age. Women and girls continue to be the primary targets of tech-facilitated violence, accounting for the majority of reports. Moreover, gender minority groups, particularly transgender women, have also reported targeted harassment and abuse online. DRF's Helpline, in order to provide the community with recourse and support, has tried various advocacy efforts to address the growing digital challenges they face. However, the number of complainants who identify themselves as transgender remains low, which is why the Helpline regularly checks up on the community, provides capacity building sessions, and conducts research to better address the needs of the community in a restrictive environment like Pakistan.



In Pakistan, the stigma and taboo attached to facing TFGBV leave women in particular without adequate support. Cultural and social restrictions hinder women from seeking support from family, which reinforces cycles of vulnerability. It is no surprise, therefore, that 83.4% of the cases received by the Helpline were self-reported; a majority of the women always express the desire for strict confidentiality and zero involvement of family members. At the same time, 16.2% of the total cases received were brought to the Helpline by a trusted person in the victim-survivors' circle, which exemplifies the distress and fear of consequences felt by the beneficiary in that situation. In this context, the Helpline serves as a crucial, confidential, and judgment-free space, enabling survivors to access guidance, digital support, and legal recourse while preserving their privacy, dignity, and autonomy.

Reporting Source



Additionally, in 7 cases (0.2%), callers who reached out to the Helpline did not identify themselves either as the victim or as an intermediary. choosing to keep their identity a secret perhaps due to a lack of trust and privacy concerns.

Perpetrators of Abuse and TFGBV

Male-perpetrated abuse remained the most common (1,132 cases) in 2025, while harassment by unknown or anonymous actors also increased slightly, highlighting the challenges of anonymity facilitated by fake accounts, AI-generated content, and cross-platform attacks.

Intimate partner harassment continues to be significant, with 253 cases in 2025 (up from 218 in 2024), reflecting the ongoing risks for survivors of breakups or divorces and the growing use of digital tools for monitoring and coercion. Harassment in online relationships was also reported, with 77 cases recorded in 2025. Harassment stemming from within the family was also reported, indicating that abuse within households increasingly involves digital means, with the purpose of control and coercion.

Relation Between Victim & Harasser	Stats in 2025
Ex-husbands/Ex-partners	253
Family members	56
Strangers / Unknown	386

*Ex-partner denotes a relationship where the couple is not or was not married.
*An online relationship is used to define a relationship where the couple initiated and continued the relationship via the internet and never met in person.

High-risk Individuals and Marginalized Communities

Certain populations and professions are more vulnerable to online harassment, threats, and security breaches as digital environments increasingly mirror offline social and political issues. Many of these people lack robust institutional protection and assistance, making them especially susceptible during times of crisis.

This year, the Helpline observed a significant increase in cases reported by journalists facing censorship, threats, defamation, doxxing, and non-consensual use of their personal information. A large number of these complaints came from Balochistan and Sindh, particularly from freelance journalists who rely on monetized social media platforms as their primary source of income. Many reported unexplained account restrictions, reduced audience reach, and a lack of platform support, directly affecting their livelihoods. Journalists also faced threats and coordinated harassment aimed at silencing their reporting. Women journalists were especially targeted with gendered and image-based abuse, putting both their professional credibility and personal safety at risk.

Additionally, threats rooted in religious narratives, along with AI-generated content such as fake images, audio, and videos, have further intensified risks for journalists and human rights defenders, and even artists. Media practitioners also continued to be prime targets of cyber harassment, particularly through attempts to hack their social media accounts.

Throughout the year, the Helpline continued to observe coordinated digital hate campaigns targeting transgender individuals. The transgender community, in particular, has been facing a coordinated gendered disinformation and hate speech campaign by identified actors for several years now, which keeps resurfacing.

Notably, another high-risk group that we have amplified our advocacy and engagement efforts for is the youth category, i.e., children and young adults under the age of 18. The gender breakdown within this group shows that young girls are almost 3 times as likely to be targeted than boys. We recognize that a more holistic approach is required to address this problem, and so we have taken on efforts to engage with multiple stakeholders, including law enforcement, parents, schools, policymakers, tech platforms, and, of course, both boys and girls.

Breakdown of Cases Involving High-Risk and Vulnerable Groups

88 Journalists
- 47 Women
- 41 Men

46 Activists
- 21 Women
- 21 Men
- 4 Transwomen

9 Artists
- 6 Women
- 3 Men

6 Civil Society Representatives
- 3 Women
- 3 Men

6 Government Organizations
- 1 Woman
- 5 Men

9 Lawyers

- 4 Women
- 5 Men

6 Media Practitioners

- 3 Women
- 3 Men

8 Government Figures

- 4 Women
- 4 Men

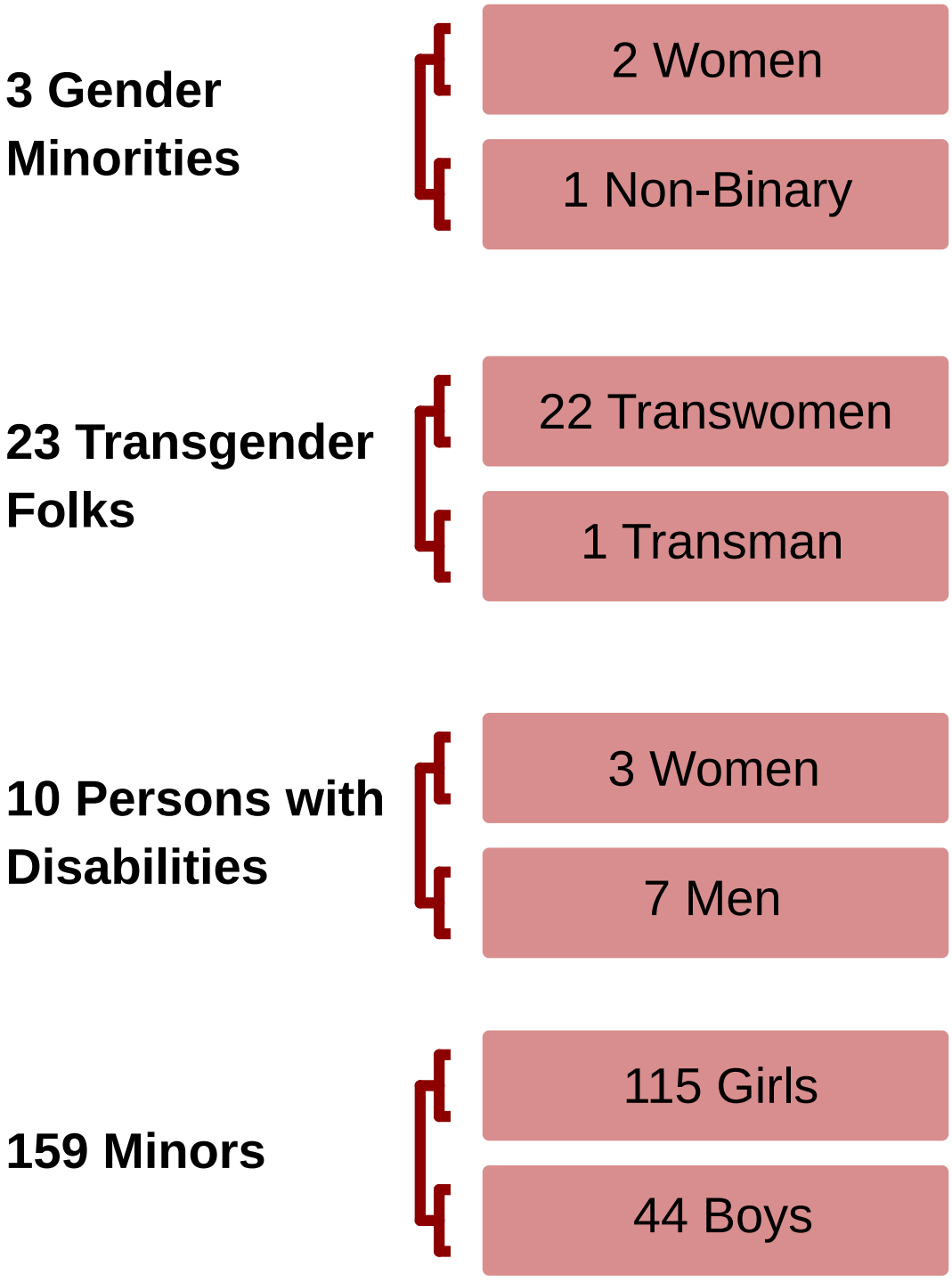
Marginalized Groups

10 Religious Minorities

- 4 Women
- 6 Men

14 Ethnic Minorities

- 1 Woman
- 13 Men


3 Gender Minorities
2 Women
1 Non-Binary
23 Transgender Folks
22 Transwomen
1 Transman
10 Persons with Disabilities
3 Women
7 Men
159 Minors
115 Girls
44 Boys

Case in Focus:
Gendered Online Attacks Targeting Journalists

Each year, the Helpline receives complaints from journalists and other public individuals who face coordinated online harassment, impersonation, and identity misuse intended to damage their credibility and silence them online. Women journalists are particularly vulnerable, as attacks often extend beyond digital spaces into professional risks, reputational harm, and threats to personal safety. States, law enforcement, and tech companies already have set systems that sometimes have little to no regard for survivors and the threats that may manifest against them due to their intersectional and diverse identities.

Case description:

The complainant identifies herself as a woman journalist who has faced repeated identity misuse and online harassment since 2021, including fake social media accounts created using her identity. Despite filing a complaint with the NCCIA, her case was closed due to alleged technical limitations. The harassment resurfaced multiple times over subsequent years, affecting both her mental health and professional credibility. She eventually sought assistance from the Digital Security Helpline, which supported her with reporting and content takedowns.

Transcription: *The first incident occurred in 2021, when fake social media accounts were created using my name and photographs. My personal data and information were misused on these accounts across different platforms. I became aware of this through people informing me and by personally coming across these fake profiles online. Over time, it became clear that this was not a one-time incident but part of a* ***recurring pattern of online harassment and identity misuse.***

My first response was to file a formal complaint with the NCCIA. Unfortunately, the experience was deeply discouraging. I expected the NCCIA to investigate the fake accounts, facilitate content takedowns, and hold those responsible accountable. ***The case remained open for nearly a year; however, it was eventually closed by the NCCIA because it lacked the technical capacity to trace IP addresses.*** *As a result, the perpetrators were not identified, and the content remained online. No meaningful support or resolution was provided.*

I later contacted DRF on my own. They provided consistent and effective support by assisting with platform reporting and content takedowns. When ***the same issue resurfaced in 2023, 2024, and again in 2025, and I discovered that my old photographs were being misused across multiple platforms,*** *DRF remained the only organization that offered practical help. While the* ***removal of images provided temporary relief, the fear and anxiety never fully subsided.*** *To this day, I avoid reverse image searches out of fear of discovering my images being misused again on new platforms.*

The incident has had a severe impact on my mental health, causing prolonged stress, anxiety, and a constant sense of fear. Professionally, it affected my work as a journalist, as fake content and fabricated narratives were used to damage my credibility and reputation. The sustained nature of the harassment made it extremely difficult to feel safe both online and offline.

I strongly believe that my identity as a journalist played a significant role in my targeting. *I not only experienced this harassment personally but also covered similar cases. Through my investigation, I obtained data showing that several women who filed complaints under Section 20/21 of PECA with the NCCIA experienced data privacy breaches. This significantly eroded my trust and made seeking help more difficult.*

A transparent, accountable, and technically capable institutional mechanism could have significantly reduced the harm. Stronger data protection, faster response systems, survivor-centered reporting processes, and real accountability for perpetrators would help rebuild trust. At present, there is a clear gap in Pakistan, where women, especially journalists, have no reliable public institution to turn to for protection against online abuse.

Tracking Digital Threats: Platform-Specific Trends and Advocacy Efforts

The Digital Security Helpline regularly monitors platform-specific patterns of online abuse and digital security threats in order to understand the evolving nature of the digital ecosystem and the effect on users in real life. The data the Helpline collects plays an instrumental role in moving beyond incident response and striving towards prevention. Due to this, DRF's program teams have developed tailored digital security guidance and designed public awareness campaigns and capacity-building sessions, keeping in mind the needs of vulnerable groups.

While major social media platforms remain central arenas of abuse, the overall pattern of data shows a relatively lower gradual shift from concentration on a small number of dominant platforms. This may be attributed to platforms' stricter content moderation standards or even the greater likelihood of them cooperating with law enforcement.

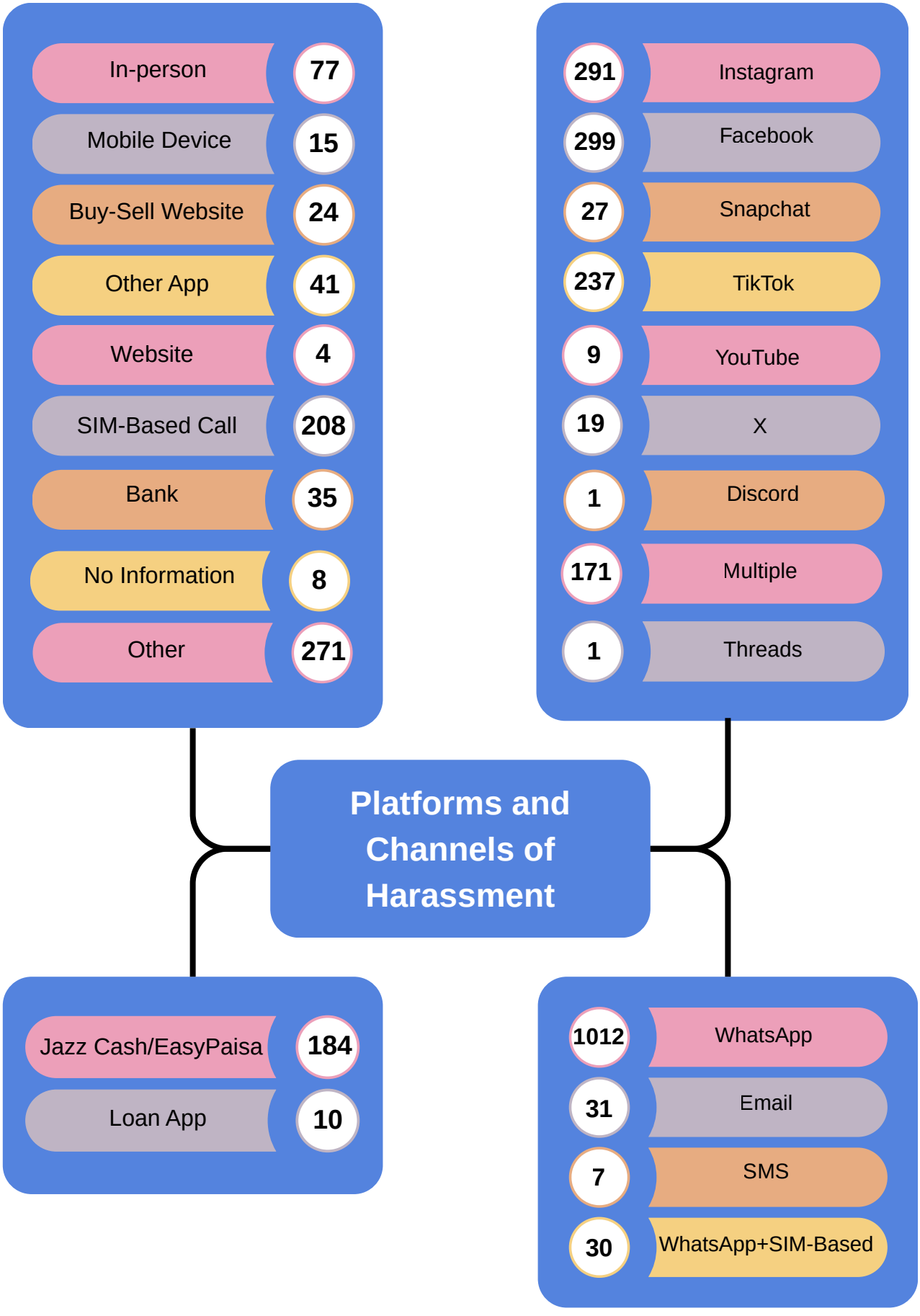
The Helpline, in 2025, documented that WhatsApp, Facebook, and Instagram together accounted for approximately 53% of reported cases, compared to 57.4% in 2024. WhatsApp alone accounted for 34% of the reported cases, highlighting the continued prominence of private and end-to-end encrypted communication in enabling sustained and difficult-to-contain forms of online abuse. For instance, features such as 'View Once' images or videos, which disappear after being accessed once, significantly limit survivors' ability to document harm and preserve evidence in cases where threatening, sexually explicit, or blackmailing material is shared.

Over the years, cases involving channels such as SIM-based calls and messages, financial platforms, and other non-mainstream applications have maintained a significant share of all reported incidents at the Helpline. The Helpline observes initial contact through messaging apps or phone calls escalating into financial exploitation, followed by threats, blackmail, and impersonation. This pattern is particularly evident in cases of TFGBV, where women are coerced into sharing personal and family information. Perpetrators then weaponize this data to sustain and deepen intimidation and force victims to comply through surveillance and manipulation.

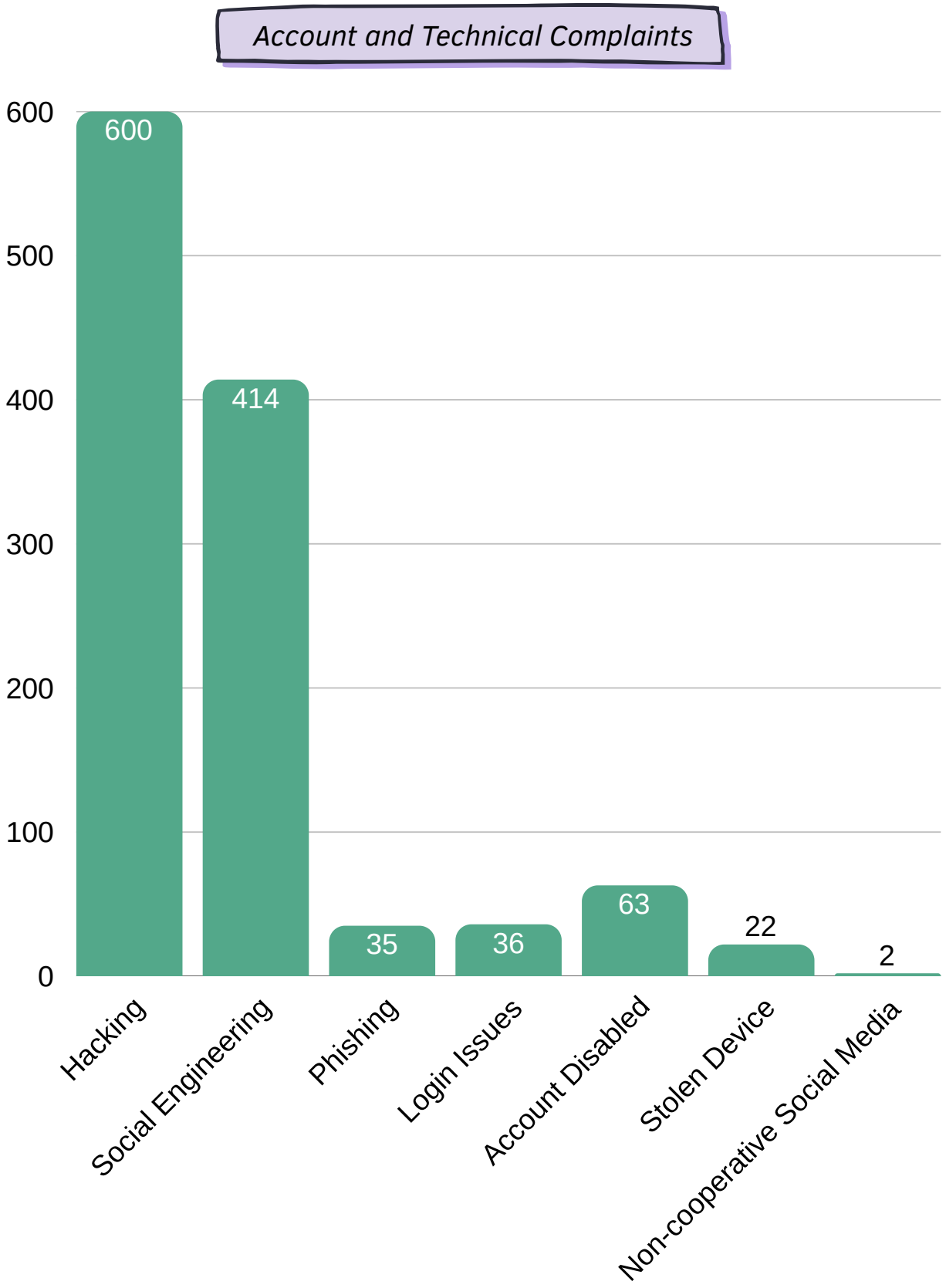
These tactics can often operate outside of formal content moderation systems, allowing perpetrators to maintain repeated contact and limiting survivors' ability to effectively block or disengage. At the Helpline, consistent reporting of these cases highlights how digital harm is increasingly sustained through direct, identity-linked communication systems rather than solely through public-facing platforms. This trend points to heightened vulnerability for users who rely on mobile-based financial services, particularly in contexts where digital and financial literacy and consumer protections remain limited. The Helpline's data reinforces the need to expand safety frameworks to address coercive exposure within financial infrastructures.

In this context, the Digital Security Helpline's role extends beyond case-specific support to function as a strategic and critical digital safety actor. As digital threats continue to evolve across technologies and infrastructures, this form of monitoring remains essential to ensure that safety interventions are informed not only by platform design but also by survivors' experiences.

Tracking Digital Threats: Platform-Specific Trends and Advocacy Efforts



Gendered Dimensions of Digital Threats: Trends and Insights



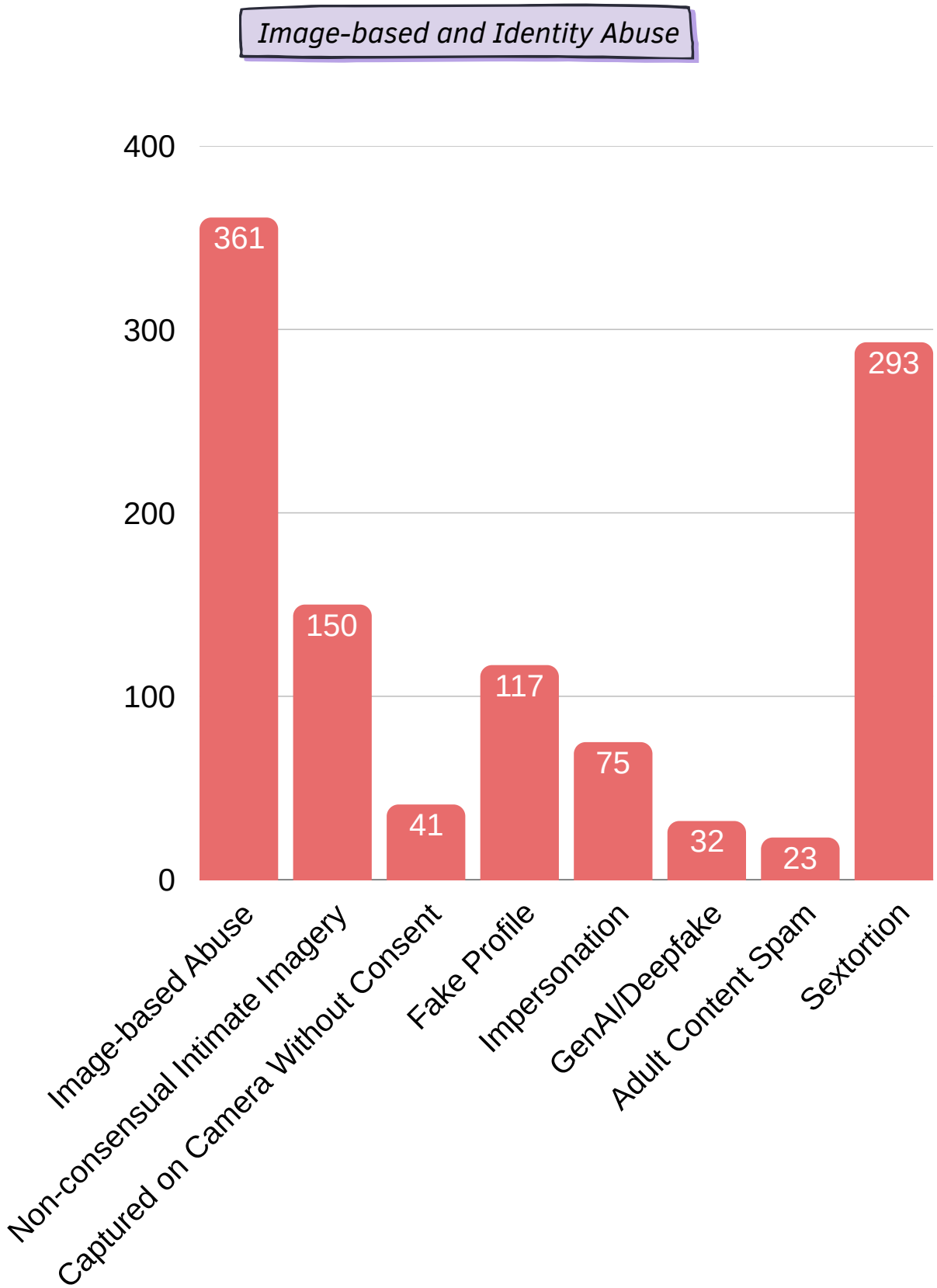
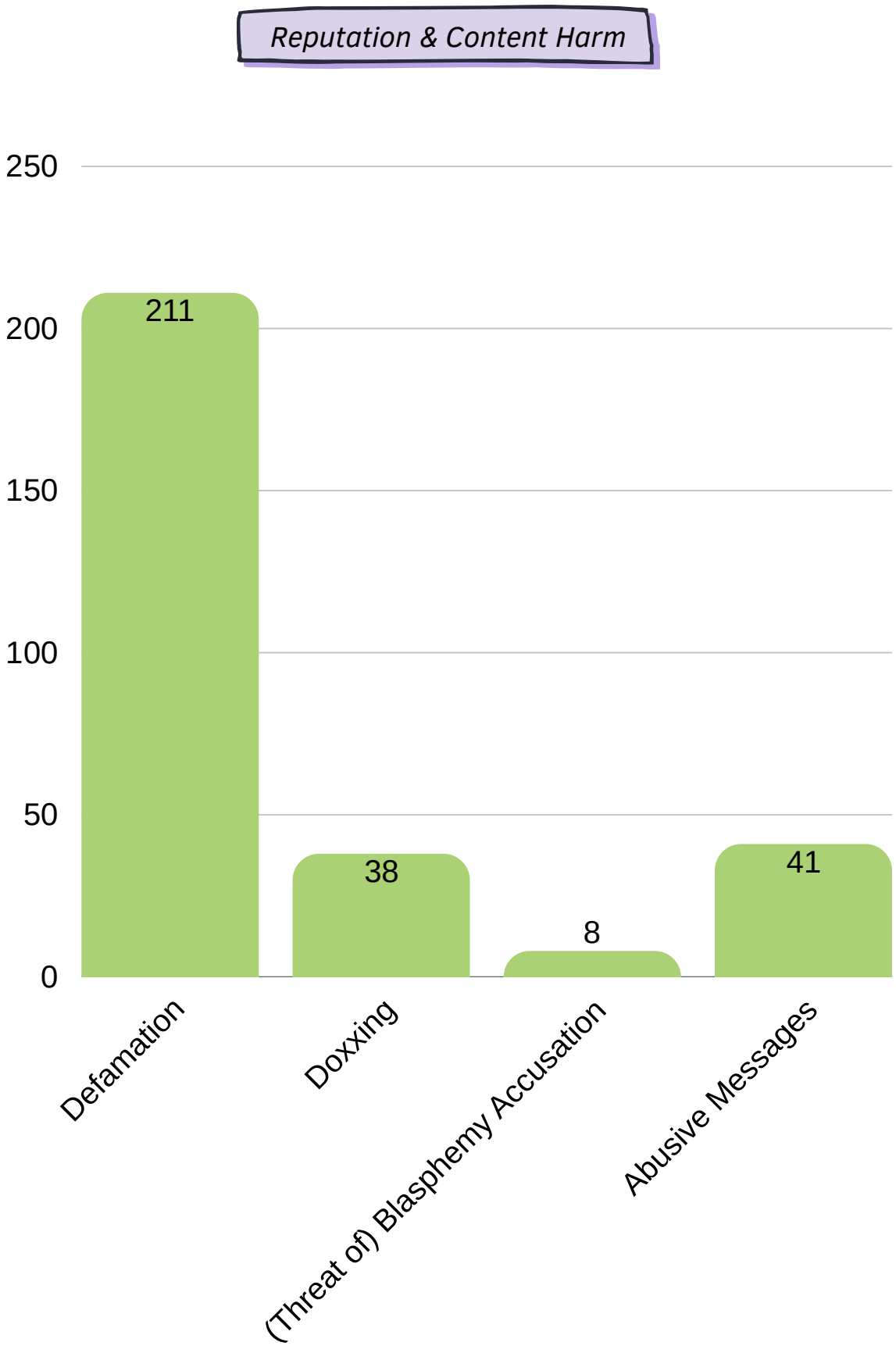
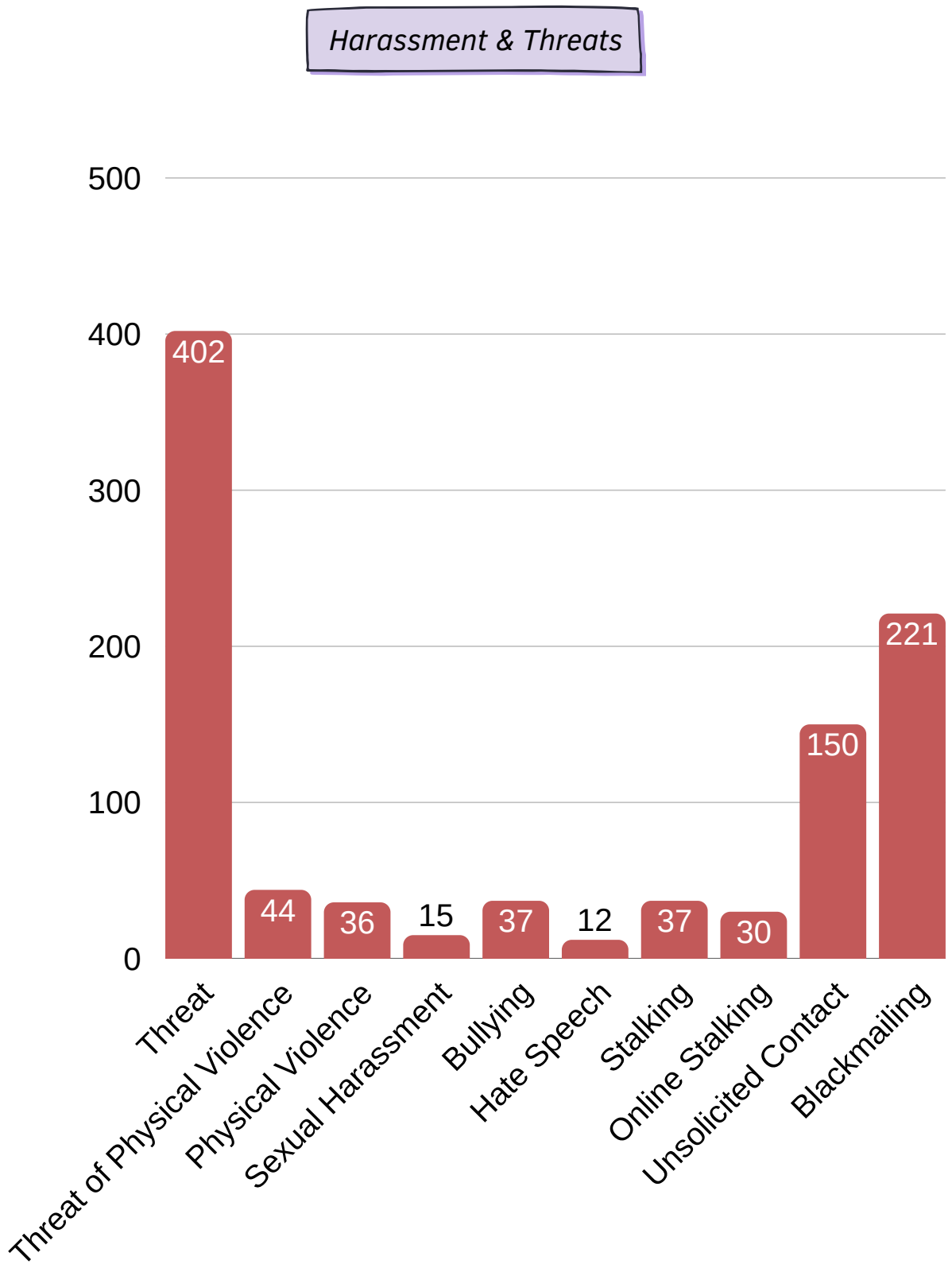
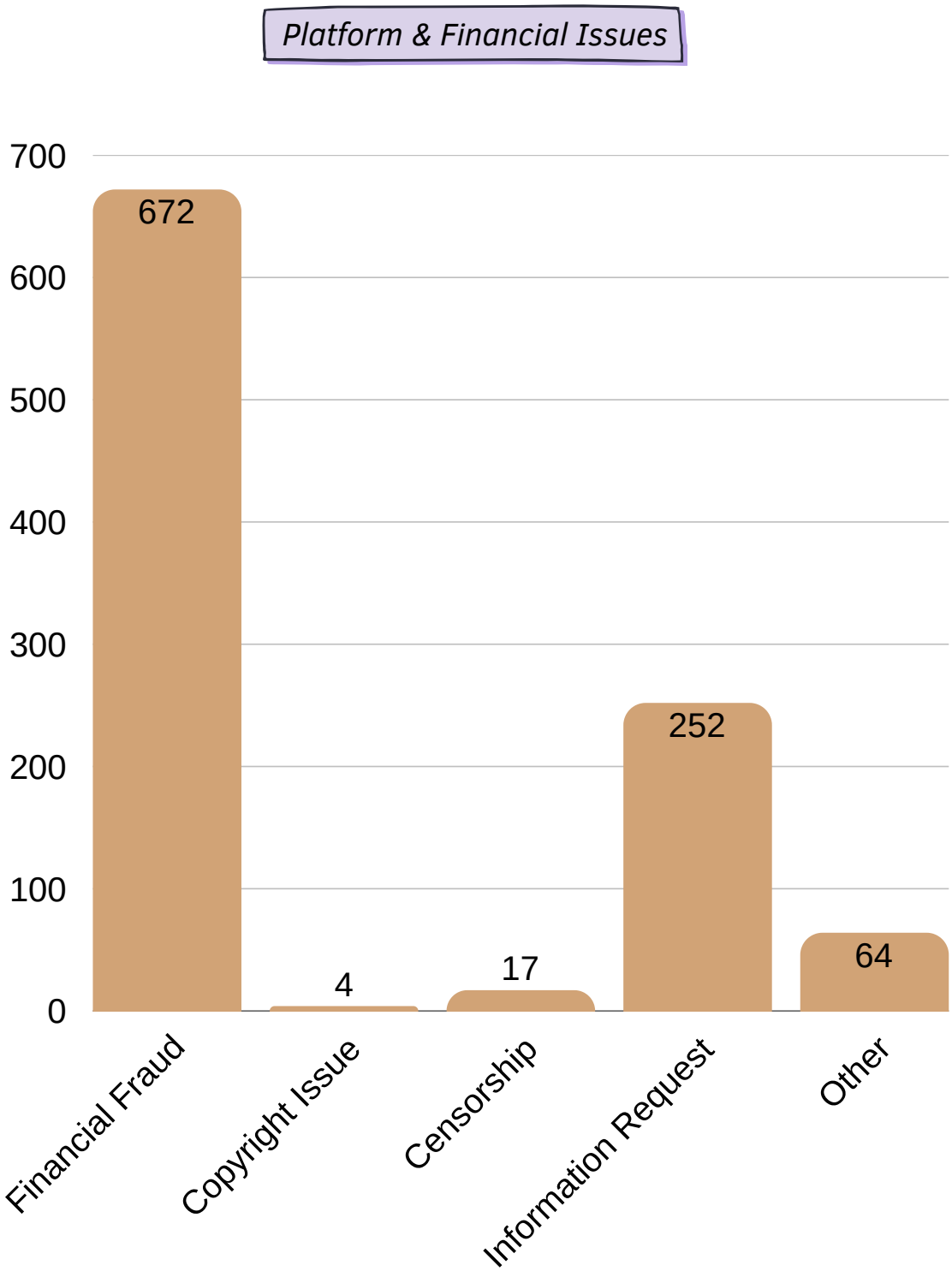


Image-based and Identity Abuse
400
300
200
100
0
361
150
41
117
75
32
23
293
Image-based Abuse
Non-consensual Intimate Imagery
Captured on Camera Without Consent
Fake Profile
Impersonation
GenAI/Deepfake
Adult Content Spam
Sextortion


Reputation & Content Harm
250
200
150
100
50
0
211
38
8
41
Defamation
Doxxing
(Threat of) Blasphemy Accusation
Abusive Messages


Harassment & Threats
500
400
300
200
100
0
402
44
36
15
37
12
37
30
150
221
Threat
Threat of Physical Violence
Physical Violence
Sexual Harassment
Bullying
Hate Speech
Stalking
Online Stalking
Unsolicited Contact
Blackmailing



Key:

IBA: Image-based Abuse

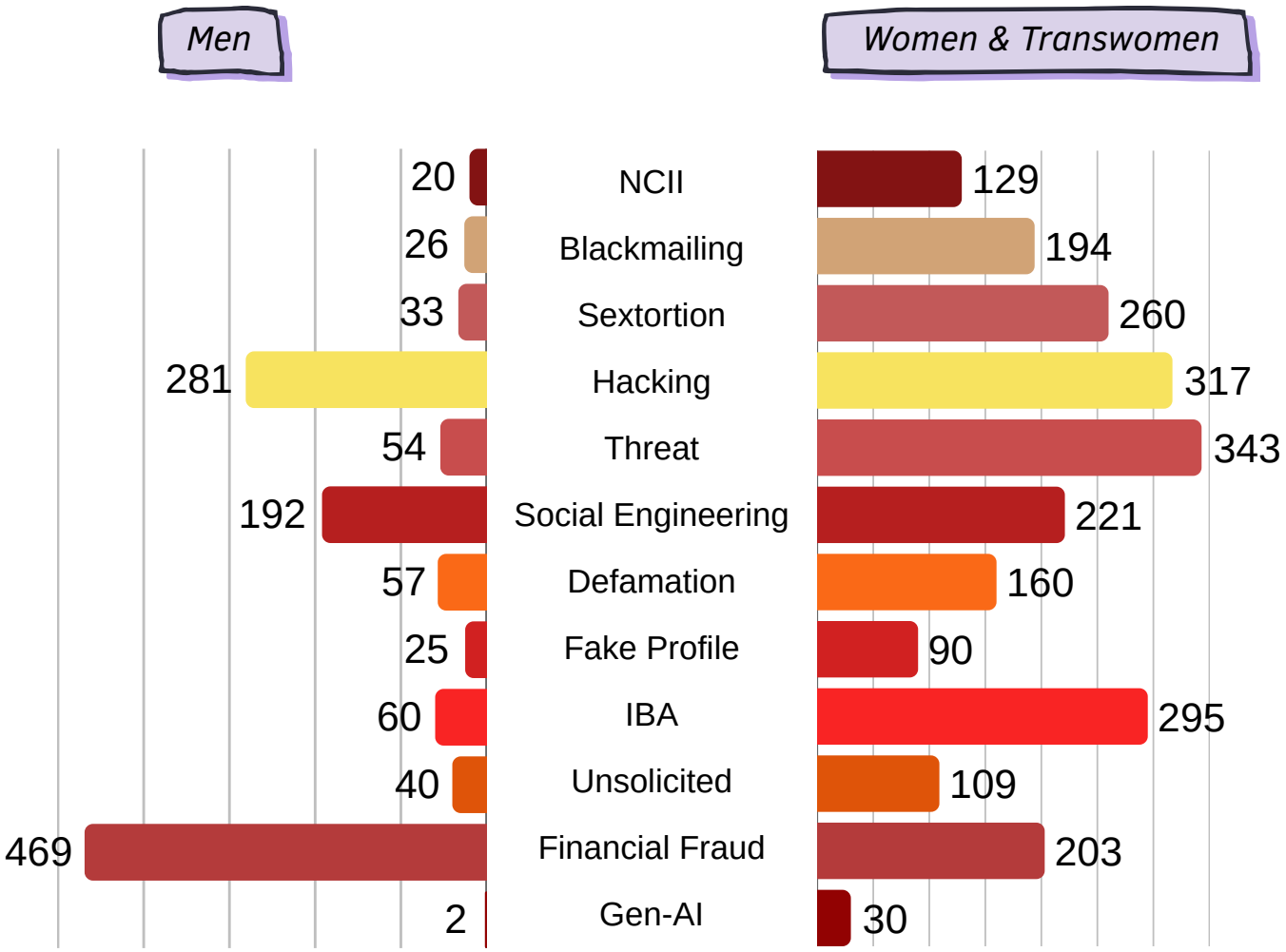
*Includes the non-consensual use, creation, or distribution of images, as well as the manipulation or editing of images without a person's consent.

NCII: non-consensual intimate imagery

NCP: non-consensual pornography sent

The Helpline addresses a wide range of online and technology-facilitated abuse. However, aggregated data alone does not fully capture the gendered dynamics and nuances behind these incidents. While the data presented above reflects the overall distribution of complaints received by the Helpline, it does not provide sufficient insight into how different forms of online harm affect people differently based on gender identity, and may not be optimal for policy making.

Gendered Patterns in Technology-Facilitated Abuse



The gender-segregated data above offers a more nuanced understanding of how technology-facilitated abuse manifests across genders. While individuals of all genders report incidents such as blackmail (including sextortion), hacking, threats, and unwanted contact, the broader trend indicates that the nature and impact of these abuses often differ depending on gender identity.

Sexualised harassment, defamation, and image-based abuse are more commonly reported by women, reflecting how perpetrators exploit patriarchal norms and honor-based social pressures. Men also report incidents of defamation, hacking, and blackmail; however, these cases are more frequently linked to financial fraud or professional harm rather than gendered or sexualised intimidation.

Transgender individuals face additional and distinct forms of online violence, including gendered disinformation, doxxing, and threats of violence. These forms of abuse often target their identity directly and differ significantly in both intent and impact from the complaints more commonly reported by men.

Non-Consensual Intimate Imagery in South Asia

DRF distinguishes between different forms of non-consensual use of imagery, including NCII, IBA, and AI-generated or deepfake content, to highlight the need for greater nuance in policymaking and platform governance, as well as in the implementation and interpretation of relevant laws.

In the Helpline's experience, IBA often involves the use of images that do not necessarily contain nudity or explicit sexual content but are still weaponized to question the honor and respectability of an individual, most often women. These patterns reflect the culturally specific ways in which image-based harms manifest in South Asia, as well as in the larger Global South. For example, seemingly ordinary photographs may be circulated with suggestive captions, emojis, or music to create sexualized implications and damage a person's reputation.

Such cases demonstrate how the meaning and impact of imagery are shaped by social norms and gendered expectations. As a result, global discussions on TFGBV, including emerging harms linked to generative AI, must take regional and cultural contexts into account when defining and addressing intimate imagery and online abuse.

In 2025, the Helpline recorded a decrease in cases explicitly involving generative AI or deepfake abuse compared to the previous year. However, this does not necessarily indicate that such harms are diminishing. While cases targeting private individuals may have declined, research conducted by DRF suggests a growing use of generative AI and manipulated imagery across various online narratives of incidents, particularly in more incidental or opportunistic contexts.

Case in Focus:

Image-Based Abuse as a Tool of Gendered Coercion and Control

Each year, the Helpline receives multiple complaints from individuals who experience technology-facilitated harassment. Survivors often face threats, blackmail, and manipulation based on their pictures. In many cases, perpetrators exploit gaps in digital literacy, legal access, and social support. Survivors frequently bear the burden of stigma, with their character questioned and their movement and device usage restricted.

Case description:

The complainant identifies herself as a woman who was subjected to sustained online harassment, manipulation, and blackmail. The perpetrator initially approached her via Facebook, building trust through conversations and emotional manipulation. Over time, he coerced her into sharing personal pictures and even demanded money under threats of exposing the images. Despite repeated intimidation, the complainant sought help through the Digital Security Helpline and ultimately filed a complaint with the NCCIA in Pakistan. While some pictures were eventually removed, threats and intimidation persisted, and the case remains ongoing.

Transcription: *The man first contacted me through a Facebook group post. After I accepted his friend request, our conversations moved to Messenger. He gradually requested pictures and swore on his mother that he would delete them. Later, he asked for my phone number. When I initially refused, he threatened to misuse my pictures, so I gave it to him. He claimed to run an orphanage and asked me to "become the mother" of a child there. I agreed and sent pictures and money for toys and support for the child over five months.*

One day, we had an argument after which I told him to stop messaging me. He then sent all the pictures back to me and threatened to upload them. ***He demanded PKR 30,000 in exchange, which I reluctantly gave him. Later, he demanded more,*** *and when I refused, he created a fake account in my name and uploaded pictures, then deleted them after payment. Eventually, he demanded PKR 100,000, which I did not have, so he uploaded my pictures again. My family and neighbors confronted me, accusing me of uploading pictures and writing inappropriate content.*

I felt completely helpless. My mother was not alive to guide me; my husband stayed silent and didn't abandon me, which I later recognized as support. Only one or two cousins defended me, while most treated the situation as gossip. I became socially isolated, avoiding leaving home. This incident completely broke me. Most of my family was watching and gossiping about me. I started staying mostly at home because I was afraid to step outside. My sisters-in-law would taunt me, saying I was unworthy of being kept at home, and even suggested that their brother should divorce me and marry again.

A friend advised me to reach out to the Digital Security Helpline. They guided me through documentation of evidence and legal channels, helping me navigate NCCIA procedures and pursue action against the perpetrator. At that time, they were the only ones who didn't blame or accuse me. They consoled me when I was crying so much. My friend's brother, who was a lawyer, was also helping me through all this. Initially, NCCIA did not take the case seriously. They said I would have to wait 15 days to go and then 15 days more to get time for follow-up. ***I went to NCCIA again and again but was told to come back later for one reason or another.*** *I used to wait the whole day, but was told the officers were on leave with no indication of when they would come back. I asked the people around me how long they had been dealing with their issues and visiting NCCIA; they said two years. I felt my courage break, but my lawyer intervened again and pressured NCCIA to take action, but still, the matter was not resolved. The lawyer contacted the perpetrator directly and threatened him with legal consequences. After that, the perpetrator deleted the images but continued threatening my family and me, saying he would come to my house and harm my family. He threatened that I would neither live nor survive peacefully.*

This harassment deeply affected my emotional and psychological well-being. ***I experienced extreme stress, fear, and anxiety,*** *and my daily life and interactions were harmed. The prolonged blackmail and humiliation also strained my family relationships. I have sought counseling to cope with ongoing trauma. I wish I could erase these two to three years from my life, but I cannot. My regret and shame prevent me from finding peace.*

Content Takedown and Escalation Resolutions

The Digital Security Helpline has maintained its escalation channels with multiple social media platforms over the years to report harmful content and support survivors facing serious online harms. In cases where the self-reporting mechanisms are unavailable, frustratingly ineffective, or result in vague outcomes, the Helpline sends in requests to action content or accounts that violate platform policies and pose significant risks to survivors. Content that was escalated during the reporting period primarily included IBA, bullying and harassment, impersonation and fake profiles, defamatory content, and account recovery requests for vulnerable and marginalized individuals.

The Helpline also advocated for cases that were outside the scope of available reporting channels, particularly account recovery requests on platforms with strict escalation criteria. In such instances, the Helpline submitted additional evidence, such as demonstrating the ineffectiveness of self-reporting mechanisms and documenting the ongoing online and offline harms experienced by complainants. This approach was necessary to ensure that individuals at heightened risk were not left unaccounted for due to platform regulatory procedural limitations.

In 2025, the Helpline initiated a total of 221 escalations, reflecting the continued prevalence of online abuse and the limitations of standard reporting mechanisms. Platforms under Meta's umbrella (Facebook, Instagram, and WhatsApp) collectively accounted for the highest number of escalations (133 cases), highlighting both their centrality in users' digital lives and their role as sites with more frequent harm. This figure also includes 17 cases (categorized under 'multiple' below) involving the cross-posting of the same links across Meta platforms, which amplified the spread of the harmful content.

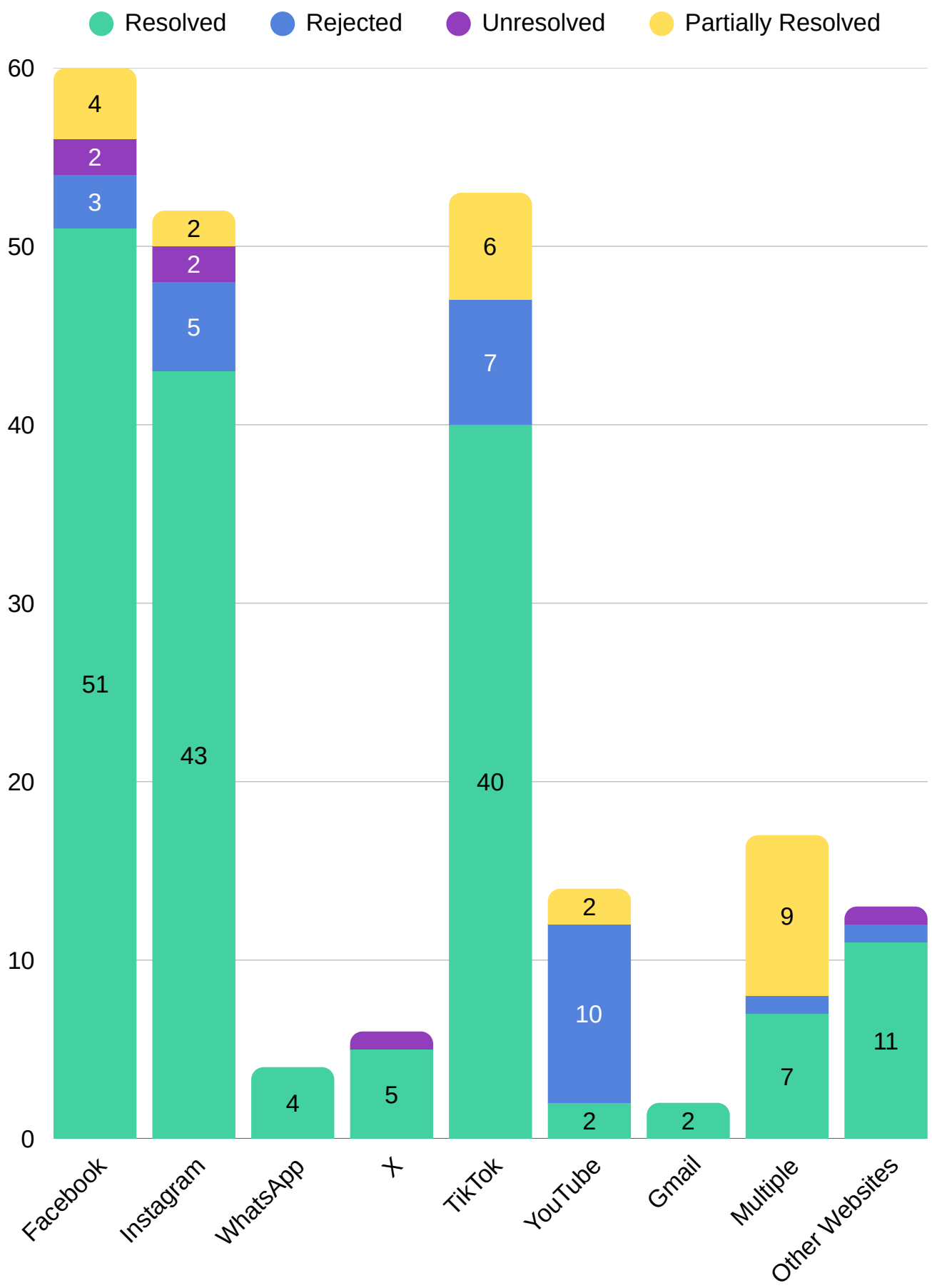
Resolution rates and response times varied widely across platforms. TikTok resolved the majority of escalations with an average response time of 1.6 days. Among Meta platforms, only WhatsApp showed relatively prompt responses, with all escalations resolved within an average of 1.5 days, including instances of same-day resolution. Other Meta platforms exhibited relatively inconsistent response patterns. Facebook escalations averaged 5.4 days, while Instagram recorded the longest response times among major platforms, averaging 6.1 days.

Based on our interactions with social media platforms, the efficiency of responses to Trusted Partners is typically measured through median resolution times; to ensure greater alignment between Helpline data and platform reporting, both median and average resolution times are presented in this report. However, the Helpline team also wants to stress that median figures do not fully reflect the full extent of survivor experiences. In practice, response times varied widely, with some cases extending from 28 to 90 days or longer. These delays are highly concerning in the case of gendered harassment, where timely intervention is critical in preventing life-threatening consequences, particularly for women.

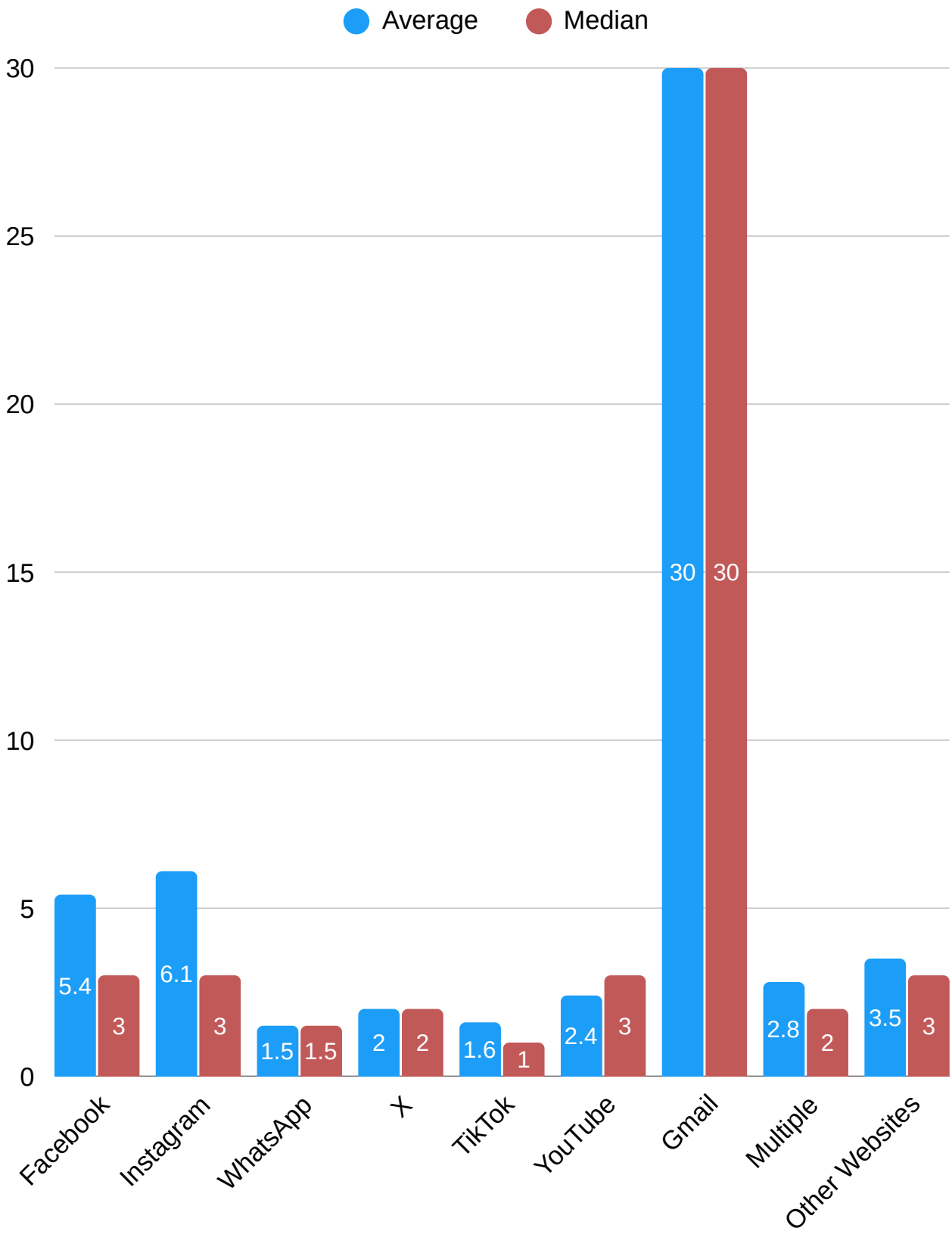
YouTube continued to present significant challenges, with a high proportion of escalations being rejected despite being aligned with the platform's policies. Even after repeated follow-ups and the provision of additional contextual information, including violation of local laws, the platform typically issued standardized responses indicating that the content did not violate its guidelines. These responses lacked sufficient clarity on the criteria applied or the manner in which contextual and cultural factors were considered while making a decision, resulting in negative results. This pattern raises concerns both about the platform's regulatory mechanisms and the adequacy of existing policies in addressing region-specific harms, particularly within South Asian contexts. The persistence of such responses underscores the need for policy frameworks that are more inclusive of diverse cultural and socio-political climates.

It is important to note that escalation outcomes did not always reflect a single interaction with platforms. In several cases, initial escalations resulted in rejections or partial resolutions. In such instances, the Helpline played the role of an active advocate rather than just a reporting intermediary to bridge the gap between platform policies and their enforcement. While escalation channels provide avenues to advocate for survivors, this responsibility should not rest only on civil society actors. The resulting back-and-forth communication can prolong response times for complainants, delaying timely protection in cases of ongoing harassment.

Escalation Statistics



Escalation Response Time (Days)



Caring for Caregivers: Supporting Incident Response Analysts

Holding space for another person's distress requires emotional presence, patience, and care. In several moments of crisis, incident response analysts may be the sole people willing to listen without judgment, to treat someone's vulnerability as sacred, and to respond with empathy and compassion. This quiet, relational labor is often invisible, yet it forms the backbone of effective support work on the Helpline. Over time, this sustained exposure to others' trauma can accumulate in the form of secondary traumatic stress for Helpline analysts. Research[22] conducted on call handlers and crisis line volunteers indicates that a substantial proportion of such professionals experience mental health strain. Around 28% report depressive symptoms, approximately 17.8% experienced signs of Post Traumatic Stress Disorder (PTSD), 17.2% reported anxiety symptoms, and similar proportions report emotional fatigue and stress-related challenges. Recognizing and caring for caregivers is therefore an essential component of sustainable service delivery.

Understanding the Emotional Experience

To gain insight into the experiences of Helpline analysts, a brief reflective assessment was conducted with an incident response analyst who has been working at a Helpline for around 5 years. The assessment was carried out through a 5-item Likert scale with open-ended, qualitative questions. The scale ranged from 1 ("Strongly Disagree") to 5 ("Strongly Agree") and addressed emotional impact, coping capacity, and perceived support. The scale items included:

22. Osório, C, S Talwar, S A M Stevelink, H K Sihre, D Lamb, and J Billings. 2024. "Systematic Review and Meta-Analysis on the Mental Health of Emergency and Urgent Call-Handlers and Dispatchers." Occupational Medicine, November. https://doi.org/10.1093/occmed/kqae104

Statement	Score (1-5)
I feel emotionally affected after handling challenging cases.	5
I feel equipped to manage my emotional responses during calls.	4
I find moments of recovery after difficult interactions.	2
I am able to maintain balance between my work and personal well-being.	4
I feel supported in managing the emotional aspects of my role.	4

Scale: 1 = Strongly disagree | 2 = Disagree | 3 = Neutral | 4 = Agree | 5 = Strongly agree
Alongside the brief quantitative scale, the analyst participated in open-ended questions exploring her emotional health, experiences of distress during calls, coping strategies, and everyday practices that support recovery and well-being.

1. Describe a call that was emotionally challenging. How did you manage it?
2. What strategies help you recharge and care for yourself?
3. Are there particular practices or routines that support your well-being at work?

Insights from the Analyst

The Incident Response Analyst reported feeling strongly emotionally affected after handling challenging cases (5/5). She described moments when callers, particularly young women, cry during calls, leaving her feeling powerless: “I feel helpless that I couldn’t do more." In cases where people are extorted out of their money, it is especially difficult for her, as she empathizes personally with the effort it takes to earn money: "People lose so much money and are unable to do anything." These accounts illustrate how the work does not remain abstract; it is felt and carried.

At the same time, the analyst indicated feeling equipped to manage her emotional responses during calls (4/5). Over time, she has developed cognitive and professional boundaries that help her stay grounded. As she explained, “I remind myself that I did what was within my control to the best of my abilities." Recognizing the limits of her role—"I am not in charge of the law"—helps her maintain perspective and provide structured, steady support even in distressing situations, reflecting her growing emotional regulation and clarity regarding her role.

However, her score for finding moments of recovery between difficult interactions was lower (2/5), suggesting that emotional processing time remains limited. The fast pace of calls and the accumulation of intense stories can make it hard to fully reset before the next interaction. While she continues to function effectively, this reduced recovery space indicates an area where additional breaks or decompression opportunities could further strengthen emotional well-being.

Encouragingly, she indicated a higher work-life balance (4/5) and feeling supported (4/5). These scores align with her evolving self-care practices. Earlier in her career, she described overextending herself, skipping breaks out of guilt and fear of missing out on an emergency call. Over time, she learned to set healthy work boundaries: “I leave office work at the office so that I can focus on myself and my family." She now talks through difficult moments with colleagues, shares concerns openly, and steps away when needed. Peer conversations and informal check-ins serve as important sources of normalization and support. As she reflected, caring for herself enables her to care for others: if she is not well, she cannot guide callers effectively.

Her reflections portray that emotional labor is real, ongoing, and actively managed. The work touches her deeply, yet she has cultivated resilience through boundaries, peer support, and meaning-making. This underscores an important principle for Helpline settings: supporting caregivers is not only protective for staff but also strengthens the consistency and compassion of care provided to those who reach out in crisis.

Insights into Reach and Trust

We continuously monitor how users connect with the Helpline to understand our reach, credibility, and the effectiveness of our digital security services. In 2025, several key patterns emerged:

Social media as the primary gateway: 75% of callers first became aware of the Helpline through social media platforms, highlighting the Helpline's strong digital visibility and the importance of leveraging online channels to reach at-risk communities.

Direct connections through DRF networks: 4.43% of individuals accessed the Helpline by contacting team members or through our established community networks, emphasising the value of grassroots engagement and survivor-centred outreach.

Institutional referrals: 14.77% of beneficiaries were referred by various government and NGO Helplines, including the local police Helpline. This reflects both our legitimacy as a trusted partner in digital security and the gap in awareness among those facing online threats, highlighting the ongoing need for public education on reporting mechanisms.

Overall, these insights reveal that our robust web presence and digital word-of-mouth recommendations demonstrate the dependability and trustworthiness of our assistance. Strengthening all channels ensures that survivors of technology-facilitated abuse can reach support quickly, confidently, and safely

Since follow-ups make up a sizable portion of our support, the number of occurrences reported does not accurately reflect the Helpline's workload. 25.8% of all calls were follow-ups, demonstrating our continued dedication and the amount of time we devote to each case in order to get the best possible outcome.

However, our stringent confidentiality policies often prevent us from initiating contact with beneficiaries unless specifically authorised; assessing absolute impact, therefore, tends to be difficult. Subjective case resolutions may also exist; some beneficiaries might find a short-term fix adequate, while others need ongoing supervision.

We also poll select beneficiaries to get their direct input. Small sample numbers, callers' uneven access to technology, and incomplete responses dependent on individual comprehension are some of the approach's drawbacks. To continuously improve our services based on actual user experiences, we are actively improving our feedback collection techniques (in Urdu and English) to make them more inclusive, representative, and instructive.

Impact Survey and Analysis

Q1. Which platform did you contact?

Helpdesk email: 10 (25.6%)
Helpline: 15 (38.46%)
Social media: 13 (33.33%)
Not answered: 1 (2.5%)

Q2. How soon did you receive an initial response?

A few minutes: 24 (61%)
A couple of hours: 8 (20.5%)
1-2 days: 4 (10.2%)
Not answered: 2 (5.1%)

Q3. Do you identify as any of the following:

Activist: 6 (15.38%)
Civil society: 2 (5.1%)
Journalist: 10 (25.64%)
Regular caller: 11 (28.2%)
Not answered: 3 (7.6%)
Student: 2 (5.1%)
Musician: 1 (2.5%)
Religious Minority: 3 (7.6%)
International civil servant: 1 (2.5%)
Pakistani army employee: 1 (2.5%)

Q4. Did you receive any digital safety advice or help with digital/social media platforms?

Yes: 37 (94.8%) (includes situations where the case did not immediately need digital security assistance, but perhaps legal support)
No: 2 (5.1%)

Q5. Did the digital help you received reduce the risk you were facing?

Yes: 37 (94.87%)
Not answered: 2 (5.1%)

Q6: Did the digital assistance you received help in building short or long-term capacity to protect yourself online?

Yes: 35 (80%)
Long term: 1 (2.5%)
Not answered: 3 (7.6%)

Q7: Did you receive digital advice beyond what was required at the time, e.g., tips to protect yourself in the future?

Positive: 23 (58.9%)
Negative: 1 (2.5%)
Not answered: 14 (35.8%)
No answer: 1 (2.5%)

Q8: Did you receive any legal guidance or help with how to contact law enforcement?

Yes: 21 (53.8%)
No: 14 (35.8%)
Not answered: 4 (10.25%)

Q9: Did you choose to pursue legal action if necessary?

Yes: 15 (38.46%)
No: 18 (46.15%)
Not answered: 5 (12.82%)
Legal action was not needed: 1 (2.5%)

Q10: Did you feel more confident seeking legal help after speaking with the Helpline?

Yes: 30 (76.92%)
No: 4 (10%)
Not answered: 5 (12.82%)

Q11: If you spoke on the phone with a Helpline Associate, did you feel emotionally supported?

Yes: 28 (90%)
No: 2 (5%)
Maybe: 1 (2.5%)
Didn't speak on phone: 3 (7.6 %)
Not answer: 5 (12.82%)

Q12: Have you ever recommended the Helpline to someone else?

Yes: 27 (69.2%)
No: 8 (20.51%)
Not answered: 4 (10%)

Our beneficiaries' experience with the Helpline

1. The associate was very sweet. I felt that she understood my situation, and it was very relieving for me to talk to someone from Instagram, which definitely gave me hope that everything might work out.

2. Behatareen tajurba raha kyoonkey unhone ne meri forun madad ki or agley hi din mera masla hal hogya!

3. It was the only hope. I am glad I reached out to the Helpline. Will refer to others facing similar challenges

4. They are feeling the pain and stress I was going through.

5. It was good. The associate listened to me patiently. Guided me properly. Very supportive.

In the face of emerging threats and evolving technology being used to put already vulnerable folks at risk, the Helpline ensured that the quality and efficiency of its services did not dip. A poll conducted by the Helpline showed a 100% satisfaction rate with the information provided by the Helpline. All 39 respondents also agreed that they felt supported and encouraged after contacting the Helpline.

More feedback from our beneficiaries

1

Your guidance and intervention have provided great relief to my family and me. We are grateful for the important work you are doing to protect individuals from online harassment and to promote digital safety.

Sister, thank you so much for your support. Hum apne mil ske Jo hmari help kre but matter solve hogya hay ab apko us ko report kernay ki zrurat nhi hay.

2

3

I am glad that I found you guys, who helped me so kindly and supported me throughout

I appreciate the time and effort taken to help me regain access to my page. Your support has been instrumental in minimizing the impact of this incident. Thank you for your dedication to addressing cyber harassment and providing support to those affected. Your work makes a significant difference.

4

5

I’m incredibly grateful to the DRF for stepping in when defamatory, exaggerated videos of me were uploaded without my consent. I had no idea what steps to take, and having a Helpline this supportive and understanding truly made me feel protected.

I was so worried, and it scared the devil out of me when I found all my Meta accounts were suspended, but thanks to the very efficient and very fast DRF team for escalating my complaint and getting them recovered quickly. DRF team members were super amazing. I am highly thankful to them.

6

7

It's a big blessing for every woman in Pakistan that DRF exists, and I personally contact them many times, just like my home organisation, and they are always ready to console and help.

Thank you for the guidance. It was your team that gave me the confirmation regarding where the cyberattacks were coming from. Saved me from speculation and pointing out any innocence. I deeply appreciate the initiative taken to launch this NGO. Last but not least, I can't express my gratitude enough to the associate for her dedication and for her active listening skills.

8

Recommendations

Law Enforcement

1. Increasing Technical Capacity and Resource Allocation

The growing need for cybercrime necessitates greater resources for the NCCIA (or any new investigative agency). Increased funding should be set aside to develop and strengthen forensic labs, recruit and educate more female officers, and enhance response systems in light of the increase in TFGBV cases. Officers need ongoing technical training in digital forensics, evidence gathering, and new trends. Enhancing investigative capacities through cooperation with foreign partners will guarantee that Pakistan's law enforcement organizations are prepared to successfully handle intricate cybercrime cases.

2. Handling Cases in International Courts

Many cybercrime cases include offenders from outside Pakistan, yet the NCCIA is unable to prosecute them. Although the NCCIA is empowered to deal with cross-border cybercrimes under Section 1(4) of PECA, actual enforcement is still difficult. The government must designate specialised officers in each branch who are trained in international law and define "international cooperation" in accordance with Section 42 of PECA to resolve this. Increasing diplomatic ties for cybercrime collaboration will hasten the prosecution of offenders who operate outside of Pakistan's boundaries.

3. Improving the Complaint Portal Online

Modernising the NCCIA's online complaint system is necessary to increase its usability and accessibility. Identity verification tools for online enquiries should be incorporated into an upgraded site so that victims can pursue justice without needless red tape. Protocols should be defined and implemented for the maximum time taken to respond to and update the complainant. The NCCIA helpline should be made operational and effective in providing procedural information to the general public.

4. Strengthening Reporting Mechanisms for Minors

NCCIA should establish a clear and accessible mechanism that allows minors to report cases with the support of any trusted adult, such as a relative (including cousins), teacher, school counsellor, or family friend. They should also be supported in being able to file a complaint without the need for traveling long distances, as it makes it culturally, logistically, and financially unviable. Such a framework should prioritise confidentiality, child protection principles, and the best interests of the minor.

5. Improving Case Follow-Up and Communication Mechanisms

Complainants have reported difficulties in securing follow-up meetings with Investigation Officers (IOs), being unable to meet the assigned officer despite travelling inter-city for the appointment, and messages and calls to the IO being unanswered. To address this frustrating communication gap, NCCIA should introduce a formalised follow-up system that includes timely case updates, responsive communication channels, and clear accountability measures for assigned officers. Establishing a digital case-tracking system, or a centralised complaint update portal, could significantly improve transparency and survivor trust. Ensuring consistent and accessible communication is essential to making the reporting process supportive rather than burdensome.

6. Enhancing Police and Cybercrime Unit Coordination

In cities without the NCCIA, local police stations can now handle cybercrime-related cases due to recent PECA amendments. The NCCIA must create explicit guidelines instructing police personnel on how to handle cybercrime accusations with compassion and effectiveness in order to guarantee that survivors receive the assistance they require. Police departments must designate focal points for cybercrime cases who are knowledgeable about current trends in cybercrime and capable of offering advice on and resolving simple cybercrimes. In order to lessen jurisdictional confusion and avoid sending survivors back and forth between agencies while seeking justice, these focal points should guarantee improved collaboration between the NCCIA and local law enforcement. In their role, they should also prioritize strict confidentiality and privacy measures while keeping a record of cybercrime cases and data.

7. Creating a Special Unit for Cyber Harassment

The NCCIA must establish a distinct unit tasked with addressing online gender-based violence that mandates specific training in survivor care, trauma-informed response, and digital harassment. The unit should also be sensitized to the unique challenges faced by members of the transgender community and gender diverse people.

8. Protecting Survivors' Privacy and Confidentiality

Complainants’ confidentiality should be made the foundation of the system. Although Rule 9 of the PECA Rules provides protections for women's privacy in circumstances of online harassment, its application is still inadequate. To guarantee that digital evidence, case information, and personal information are safely maintained and only available to authorised staff, the NCCIA has to fortify its internal case management system.

9. Enhancing Accessibility for Disabled Complainants

People with disabilities must be able to access cybercrime offices. The absence of wheelchair ramps, accessible facilities, and working elevators presents extra challenges for many complainants. It will be easier for people with disabilities to report cybercrimes if all cybercrime agencies adhere to basic accessibility guidelines.

10. Enhancing Branches of Cybercrime Coordination

Inter-branch collaboration should be prioritized and made efficient to ensure there are no unnecessary delays in investigations. Standardized protocols across branches will also ensure uniformity and quicker processing; a centralized database for cybercrime cases should be created.

11. Offering Services for Psychological Support

Survivors of online harassment frequently suffer from extreme emotional suffering. In order to provide trauma counselling to complainants, the NCCIA must incorporate psychological support services inside its cybercrime sections. To guarantee that victims receive considerate and expert assistance, officers who handle cyber harassment situations ought to receive training in trauma-informed response strategies.

Social Media Platforms

1. Adopt Regionally Informed Moderation Approaches

In contexts such as Pakistan, online harms can have serious offline consequences, including social exclusion, violence, and legal risks. Platform moderation strategies should account for these realities and recognize that harmful narratives often spread across borders, particularly in regions like South Asia that share languages and cultural ties. Platforms should therefore adopt regionally informed moderation approaches that better address cross-border trends in abuse, harassment, and misinformation.

2. Prioritize Reports from Trusted Civil Society Partners

Digital rights organizations frequently act as first responders to online abuse and possess valuable contextual knowledge. Reports and escalations submitted by trusted partners should be treated with urgency, particularly in cases involving non-consensual image sharing, impersonation, hate speech, or sexualized threats. Platforms should ensure that trusted partner mechanisms are transparent, responsive, and time-sensitive, reducing reliance on automated responses and minimizing the need for repeated follow-ups. Clear communication and timely updates on policy or procedural changes are also essential for maintaining effective collaboration.

3. Maintain Reliable Escalation Mechanisms

Consistent and dependable escalation pathways are critical for addressing high-risk cases. Sudden institutional changes, such as the removal of advisory structures or trusted partner channels, can weaken protections and delay responses to urgent harms. Platforms should ensure that escalation systems remain stable during internal transitions and maintain dedicated communication channels with local civil society organizations, particularly in high-risk contexts.

4. Improve Reporting Tools and Response Times

Many cases reported to the Helpline require immediate intervention due to risks such as non-consensual intimate image sharing, hate speech, or threats that may escalate offline. Delays in moderation responses can significantly increase harm. Platforms should shorten response timelines for high-risk reports and ensure that escalation mechanisms remain accessible. At the same time, user-facing reporting tools must be easier to navigate and more reliable, with clearer feedback and follow-up for those submitting complaints.

5. Increase Transparency and Accountability

Platforms should publish detailed, country-specific transparency reports that include data on reported harms, enforcement actions, response timelines, and outcomes of escalations from civil society and government partners. Greater transparency is necessary to assess whether platform policies are applied consistently and whether protections are effective for groups disproportionately affected by online abuse, including women, journalists, and gender minorities.

6. Improve AI Moderation for Local Contexts

Automated moderation systems often fail to capture cultural nuance, regional languages, and local forms of harassment. This can lead to both under-enforcement of harmful content and the wrongful restriction of legitimate speech. Platforms should invest in more inclusive training datasets and moderation tools that better recognize regional languages, visual content, and context-specific threat patterns to ensure fairer and more accurate outcomes.

7. Develop Accessible Safety Resources

Platforms should collaborate with regional civil society organizations to develop practical safety resources tailored to local contexts. Guidance on privacy settings, reporting tools, and strategies to prevent online harassment should be available in local languages and accessible formats. Particular attention should be given to supporting women, youth, parents, and transgender communities, who may face heightened risks online.

8. Integrate Safety and Privacy into Product Design

User safety and privacy should be central to platform design, especially in contexts where device sharing and surveillance within households are common. Features such as anonymous reporting, comment moderation tools, privacy controls, and other protective options should be designed to enhance user autonomy and allow survivors of abuse to engage online more safely.

9. Strengthen Engagement with Global South Civil Society

Platforms should institutionalize regular engagement with civil society organizations in regions such as South Asia. These consultations should inform safety policies, escalation procedures, product design, and crisis response strategies. As policy changes made in large markets often affect users globally, platforms must consider the potential impacts on users in the Global South and ensure that safety protections remain effective across different regional contexts.

Policymakers

1. Consistency and Accessibility in Cybercrime Frameworks

Frequent structural changes to cybercrime enforcement under the PECA have created uncertainty for both complainants and investigators. Any reforms to complaint mechanisms should prioritize accessibility, clarity, and efficiency, particularly for women and marginalized communities. Rather than repeatedly establishing and dissolving new investigative bodies, policymakers should address systemic barriers that hinder investigations and case resolution. Strengthening the resources, training, and technical and forensic capacity of existing law enforcement agencies would likely lead to more effective outcomes. With the possibility of the formation of provincial cyber crime investigation units, rules and jurisdictions will need to be clearly defined, and public awareness campaigns necessary.

2. Public Education and Digital Literacy

Addressing online harassment and TFGBV requires sustained investment in public education and digital literacy. A gender-sensitive approach should be integrated into school curricula, public awareness campaigns, and community programs to promote understanding of online consent, responsible social media use, cyber laws, and digital safety. Collaboration with digital rights and gender-focused civil society organizations can help ensure these initiatives are inclusive and responsive to emerging online risks.

3. Bridging the Digital Gender Divide

Pakistan continues to face one of the largest digital gender gaps globally, with women significantly less likely than men to own mobile phones or access the internet. Targeted policies are needed to make digital access more affordable and inclusive. This includes working with mobile network operators to provide subsidized internet packages for women, expanding connectivity in underserved regions, and addressing social norms that restrict women's digital participation through community engagement and awareness initiatives.

4. Gender-Sensitive Law Enforcement

Law enforcement agencies should adopt a survivor-centered approach when handling cyber harassment cases. Regular gender-sensitization training should be institutionalized for officers, particularly within the NCCIA and police departments. These trainings should focus on the specific risks faced by women and gender minorities online and promote empathetic, professional handling of complaints. Partnerships with civil society organizations can help develop standardized training and ensure continuous evaluation of these efforts.

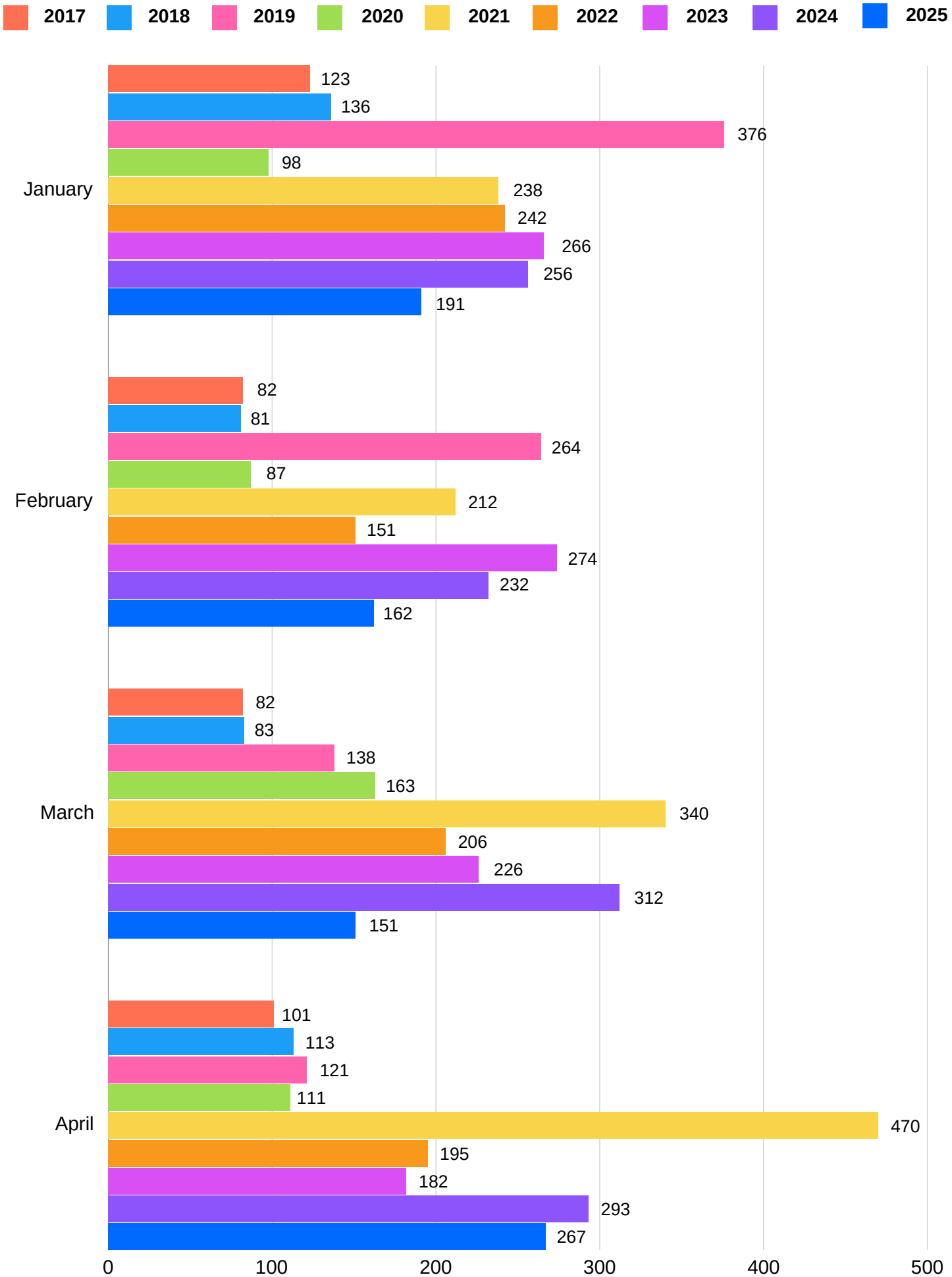
5. Strengthening Data Protection Frameworks

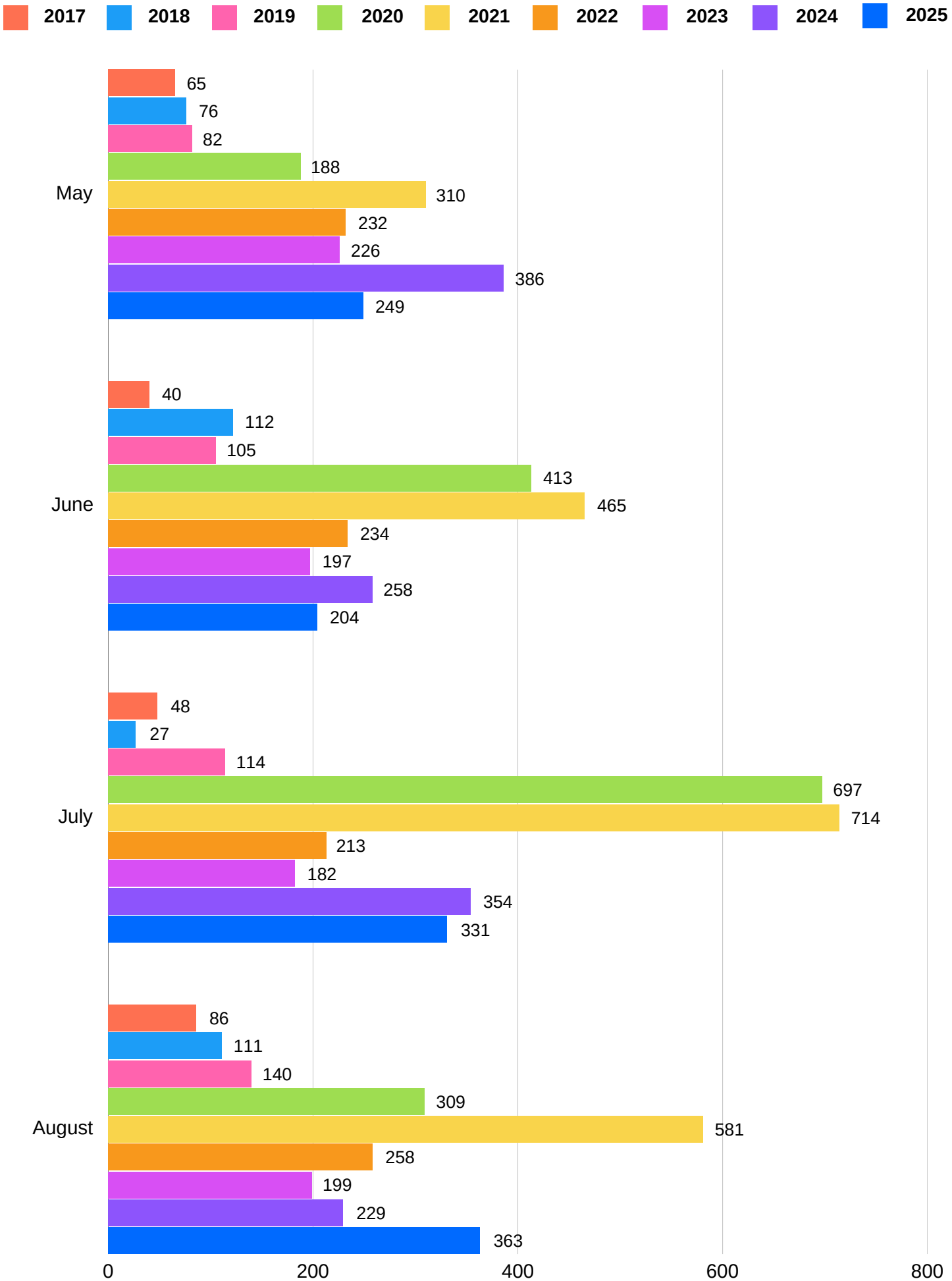
Pakistan should enact comprehensive, human rights-compliant data protection legislation to safeguard citizens' privacy and digital security. The law should establish clear standards for the collection, processing, and sharing of personal data, while ensuring transparency and accountability in how both private and public entities handle user information. The legislative process should include meaningful consultation with civil society and align with international best practices. Effective grievance mechanisms and enforcement measures must also be introduced to address privacy violations.

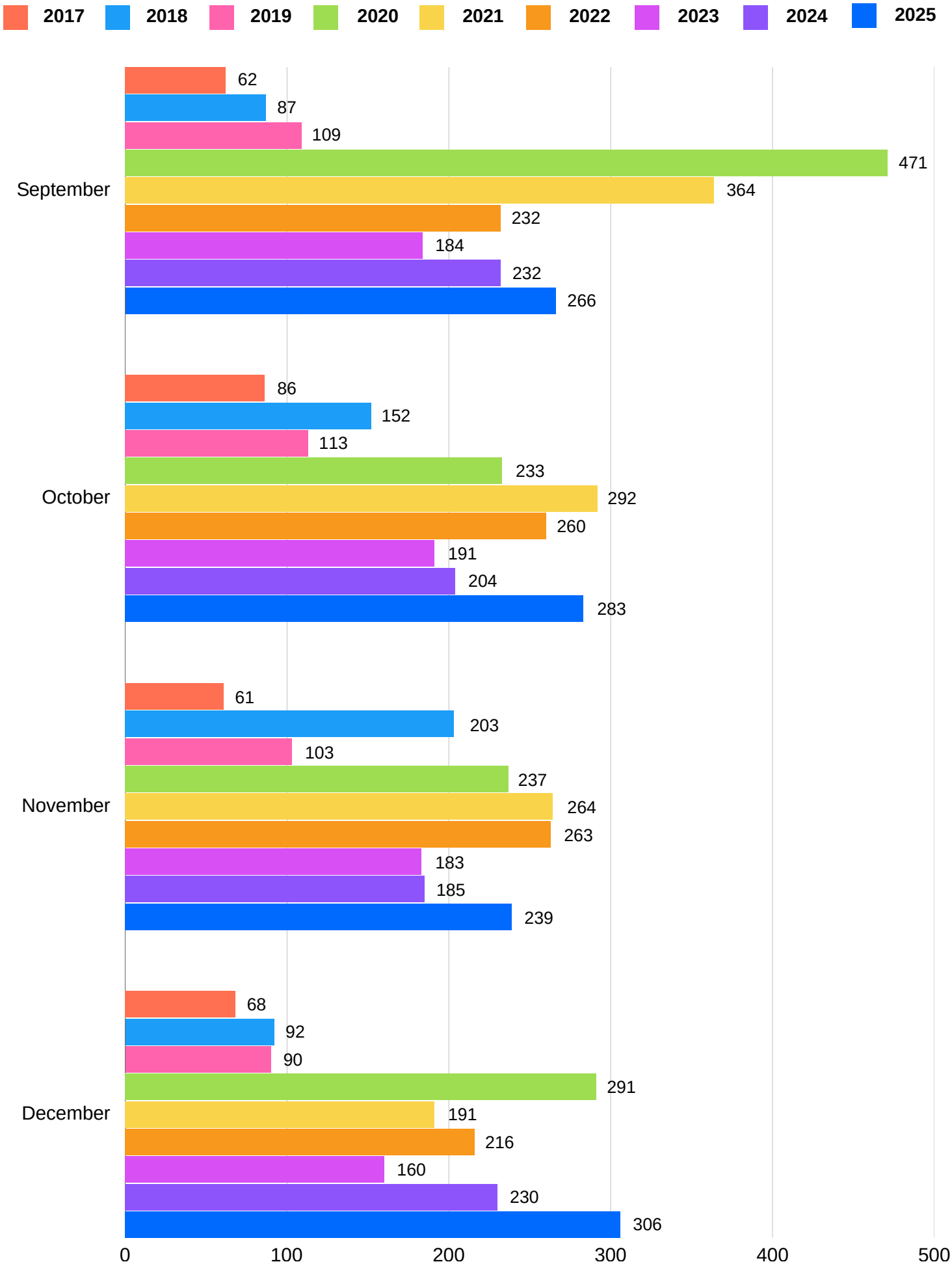
6. Supporting Civil Society and Digital Rights Work

An enabling environment for civil society organizations is essential for addressing online harms and advancing digital rights. The government should facilitate meaningful engagement with organizations working on gender equality, digital security, and online safety. Supporting research, advocacy, and survivor support services through financial and institutional mechanisms can strengthen national responses to cyber harassment and related harms.

Appendix 1


2017
2018
2019
2020
2021
2022
2023
2024
2025
January
123
136
376
98
238
242
266
256
191
February
82
81
264
87
212
151
274
232
162
March
82
83
138
163
340
206
226
312
151
April
101
113
121
111
470
195
182
293
267
0
100
200
300
400
500


2017
2018
2019
2020
2021
2022
2023
2024
2025
May
65
76
82
188
310
232
226
386
249
June
40
112
105
413
465
234
197
258
204
July
48
27
114
697
714
213
182
354
331
August
86
111
140
309
581
258
199
229
363
0
200
400
600
800


2017
2018
2019
2020
2021
2022
2023
2024
2025
September
62
87
109
471
364
232
184
232
266
October
86
152
113
233
292
260
191
204
283
November
61
203
103
237
264
263
183
185
239
December
68
92
90
291
191
216
160
230
306
0
100
200
300
400
500

DigitalRightsFoundation

"KNOW YOUR RIGHTS"

@DigitalRightsFoundation

@digitalrightsfoundation

@digitalrightsfoundation

@digitalrightsfoundation

Digital Rights Foundation

@digitalrightspk.bsky.social

@DigitalRightsPK

@DigitalRightsPK

digitalrightsfoundation.pk